联想天工 iSpirit 2924G/2924F 交换机

用户手册

声　明

欢迎您使用联想产品。

在第一次安装和使用本产品之前，请您务必仔细阅读随机配送的所有资料，这会有助于您更好地使用本产品。如果您未按本手册的说明及要求操作本产品，或因错误理解等原因误操作本产品，联想网络（深圳）有限公司将不对由此而导致的任何损失承担责任，但联想专业维修人员错误安装或操作过程中引起的损失除外。

联想网络（深圳）有限公司已经对本手册进行了严格仔细的校勘和核对，但我们不能保证本手册完全没有任何错误和疏漏。

联想网络（深圳）有限公司致力于不断改进产品功能、提高服务质量，因此保留对本手册中所描述的任何产品和软件程序以及本手册的内容进行更改而不预先另行通知的权利。

本手册的用途在于帮助您正确地使用联想产品，并不代表对本产品的软硬件配置的任何说明。有关产品配置情况，请查阅与本产品相关合约（若有）、产品装箱单或咨询向您出售产品的销售商。本手册中的图片仅供参考，如果有个别图片与产品的实际显示不符，请以产品实际显示为准。

如果您在使用过程中发现本产品的实际情况与本手册有不一致之处，或您想得到最新的信息，或您有任何问题或想法，请垂询或登陆：

咨询电话：0755-33306800
服务网站：www.lenovonetworks.com
服务邮箱：support@lenovonet.com

序列号：147001356
手册版本：V2.0

目　录

第一部份 硬件操作

第 1 章 产品综述

本章主要描述联想天工 iSpirit 2924G/2924F 交换机的前面板与后面板的组成、功能特性、所支持的标准及应用举例。本章包括以下内容:

1、产品概述
2、产品特性
3、标准协议
4、交换机前面板说明
5、交换机后面板说明

1.1 产品概述

联想天工 iSpirit 2924G/2924F 交换机是联想网络（深圳）有限公司推出的面向企业网工作组接入以及 IP 城域网小区接入应用推出的可网管支持千兆快速以太网交换设备。可为大中小型以太网 / 快速以太网 / 千兆以太网提供完美的解决方案。它具有高性能的基于策略的第二层交换能力, 用户不仅可以在其上连接工作站、服务器、路由器、交换机等网络设备，还可以将其作为主干交换机，从其他网络设备处聚合十兆、百兆、或千兆以太网数据流 。

iSpirit 2924G/2924F 交换机提供 24 个 RJ-45 的 10/100Base-T 自协商端口、2 个光电自切换千兆口和 2 个扩展接口，分别可插 1000M 光纤模块、10/100/1000 Base-T 自适应 RJ45 端口模块、堆叠模块。适用于政府、院校、金融以及其他企业工作组用户接入和运营商驻地网宽带 IP 接入。

联想天工 iSpirit 2924G/2924F 交换机的外观如图 1-1 所示

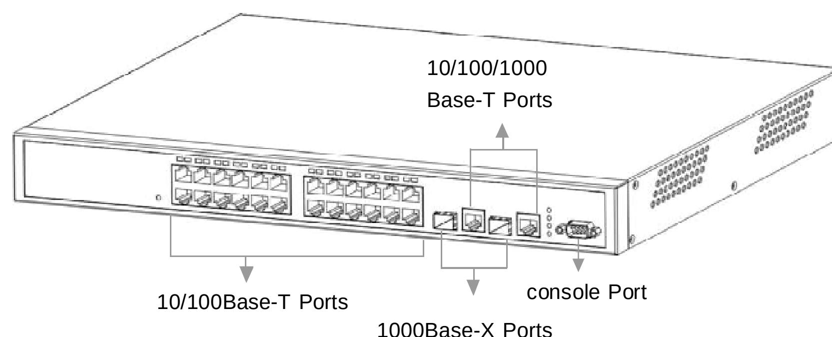


图 1-1A 联想天工 iSpirit 2924G 交换机模型

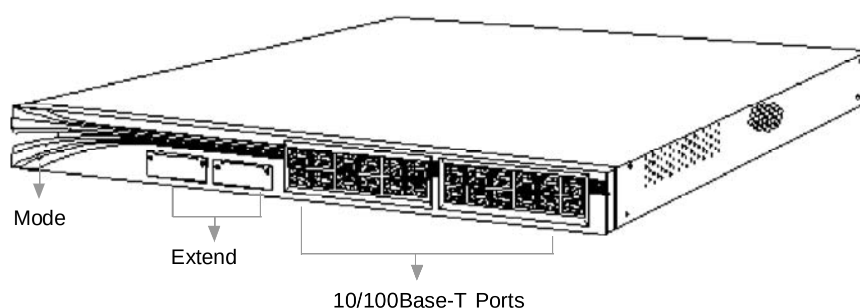


图 1-1B 联想天工 iSpirit 2924F 交换机模型

1.2 产品特性

1.2.1 产品的技术特性

10/100 Mbps 端口直连网线与交叉网线连接的自协商
10/100 Mbps 端口自协商和半 / 全双工操作
1000M 单模 / 多模光纤模块、10/100/1000Base-T 铜线接口模块
超距离网线支持能力，最长支持 CAT5 网线距离可达 140 米
自动源地址学习
8K ARL 表
提供流量控制，支持 IEEE802.3X 线端阻塞（HOL)和背压（Backpressure)
提供 4 个优先级队列，为多媒体和其它数据流提供灵活的优先级机制
网络适配器可以和端口绑定，实现安全访问
支持端口聚合，聚合最多可支持 4 组，每组最多支持 8 个速度相同的端口
基于端口的 VLAN 和基于 802.1Q tagged VLAN，支持 256 个 VLAN。
支持 STP 协议
支持 MIBII，RMON（4 种）
支持 IGMP 侦听
支持 XModem 软件升级
支持 802.1X 认证协议
支持协议 VLAN
支持私有 VLAN
支持 MAC 地址过滤
支持基于 802.1P、TOS/DSCP、MAC 地址、端口策略的 QoS 配置，灵活分配业务的优先级
支持保护 VLAN

1.2.2 产品的业务特性

1.百兆和千兆聚合技术

联想天工 iSpirit 2924G/2924F 交换机支持快速以太网以及千兆以太网的链路聚合技术，允许网络管理员将多达 8 个 10/100 端口组合到一个通道中，多达 4 个 Trunk group，将 2 个 Gigabit Ethernet 组合到一个上行链路通道中。

2.安全特性

联想天工 iSpirit 2924G/2924F 交换机支持 ARL 表的静态设置以及 MAC 地址与端口的绑定，实现对 MAC 的控制过滤，独有的 Hyper-Safety 技术,使得非法主机无法接入网络获取网络资源。

3.强大的网络管理

联想天工 iSpirit 2924G/2924F 交换机采用 Hyper-Management 技术，拥有强大和完善的网络管理功能。
(1)可以利用 Console 和 Telnet 口进行 Menu 或者 CLI 方式的网络管理配置
(2)通过基于 SNMP 的网管软件可以进行网络管理
(3)可以基于 web 的页面管理图形用户接口，操作简单，功能强大，界面直观
(4)内置多种 SNMP 的网管代理，Bridge MIB、MIB II、Entity MIB version 2、RMON MIB 和 Proprietary MIB
(5)4 组 RMON 的（1、2、3、9）网管协议（统计量信息、历史信息、告警信息、事件信息）
(6)易于软件升级设计，可以通过 TFTP 的带内（in-band）升级方法实现。

4.VLAN

联想天工 iSpirit 2924G/2924F 交换机实现的 VLAN 技术支持基于端口的 VLAN 符合通用标准 802.1Q。
联想天工 iSpirit 2924G/2924F 交换机实现了协议 VLAN。
联想天工 iSpirit 2924G/2924F 交换机实现了保护 VLAN。
联想天工 iSpirit 2924G/2924F 交换机实现了私有 VLAN。

1.3 标准协议

联想天工 iSpirit 2924G/2924F 交换机支持的标准和协议见表 1-1

表 1-1

协 议	参考文档
桥 （生 成 树）	IEEE802.1d
以太网	IEEE802.3
快速以太网	IEEE802.3u
全双工流控	IEEE802.3x
千兆以太网	IEEE802.3z
Link Aggregation	IEEE802.3ad
VLAN	IEEE802.1Q
UDP	RFC 768,RFC 950,RFC 1071
TCP	RFC 793
TFTP	RFC 783
IP	RFC 791
ICMP	RFC 792
ARP	RFC 826
Telnet	RFC 854~RFC 859
SMI	RFC 1155
SNMP	RFC 1157
MIB II	RFC 1213 & RFC 1573
Ether-like MIB	RFC 1398
Bridge MIB	RFC 1493
Ether-like MIB	RFC 1643
RMON	RFC 1757

1.4 交换机前面板说明

iSpirit 2924G/2924F 交换机前面板包含 10/100Base-T RJ-45 端口、1000Base-X 光电自切换端口、端口 LED 状态指示灯（如图 1 - 2 所示）。

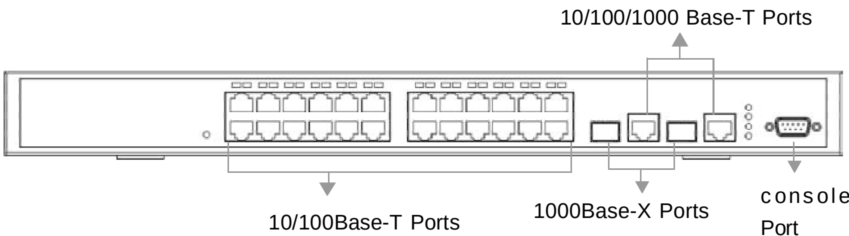


图 1-2A iSpirit 2924G 交换机前面板

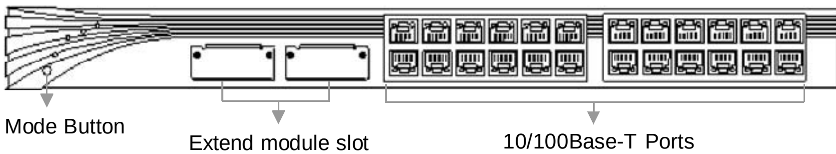


图 1-2B iSpirit 2924F 交换机前面板

1.4.1 10/100Base-T 端口

交换机 10/100Base-T 端口可以连接的网络设备的最远距离是 140 米。其可连接的网络设备包括：

➲ 10Base-T 兼容设备，如通过 RJ-45 接口和 CAT3、CAT4、CAT5 或 CAT5E 网线连接的工作站或集线器。

➲ 100Base-TX 兼容设备，如通过 RJ-45 接口和 CAT5 或 CAT5E 网线连接的高速工作站、服务器、路由器、集线器或其他交换机。

注意：

❶ CAT3、CAT4 网线只可以承载 10Mbps 数据流，而 CAT5、CAT5E 网线可以承载 100Mbps 数据流。

❷ 10/100Base-T 端口网线直连与交叉连接自协商。

可以以任意组合将交换机 10/100Base-T 端口设置成半双工、全双工、十兆或百兆端口。也可以遵循 IEEE802.3u 将端口设置成速度和双工的自协商。当端口设置了自协商后，端口会自动感知与其连接设备的速度和双工设置并通知该设备端口的性能。如果与其连接的设备也支持自协商，则交换机端口会将连接调整到最好状态（即速度设置为双方都支持的最快的速度，如果与交换机相连的设备支持全双工则双工设置为全双工)，同时把自己的状态作相应调整。

注意：根据 IEEE802.3u 的标准，自协商过程需要建立双方交互协商的连接，我们推荐用户将交换机端口以及与其连接的设备端口设置为自协商，这样可以保证交换机的自适应功能将连接调整到最佳状态。

1.4.2 1000Base-X 去电自切换端口

iSpirit 2924G/2924F 交换机自切换端口，通过一个插入 SFP 模块与光纤相连，目前支持的 SFP 模块类型及每种类型最长支持光纤长度如表 1-2 所示：

表 1-2

模块类型	介质	波长	最长支持长度
1000Base-SX	62.5um多模光纤	850nm	275m
	50um多模光纤		550m
1000Base-LX	62.5um多模光纤	1310nm	550m
	50um多模光纤		550m
	9um单模光纤		10000m
1000Base-ZX		1550nm	100000m

1.4.3 扩展模块插槽

iSpirit 2924F 交换机带有 4 个扩展模块，正面 2 个，背面 2 个。iSpirit 2924G 交换机正面带有 2 个扩展模块。所支持的模块类型有：

表 1-3

模块类型	介质	波长	最长支持长度
1000Base-TX	5类非屏蔽双绞线		100m
1000Base-SX	62.5um多模光纤	850nm	275m
	50um多模光纤		550m
1000Base-LX	62.5um多模光纤	1310nm	550m
	50um多模光纤		550m
	10um单模光纤		5000m

注意：1000 **兆光口默认模式为强制** full-1000。

图 1-3 **以** 2924F **为例说明如何将一个扩展模块(可选)插入** 2924F **交换机扩展模块插槽。**

2924F **交换机两个扩展模块插槽在机器背面。**

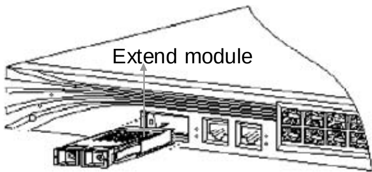


图 1-3 **将一个模块插入** 2924F **交换机扩展插槽**

1.4.4 LED 状态指示灯

用户可以通过 LED **状态指示灯监测交换机的活动和性能。模式** LED **状态指示灯、**Link LED **状态指示灯的位置如图** 1-4 **所示。**

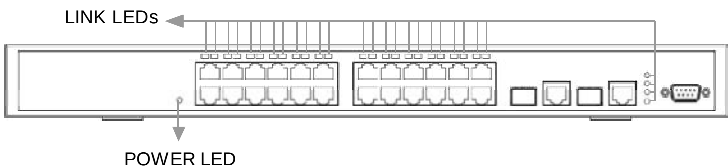


图 1-4 iSpirit 2924G **端口** LED **指示灯位置图**

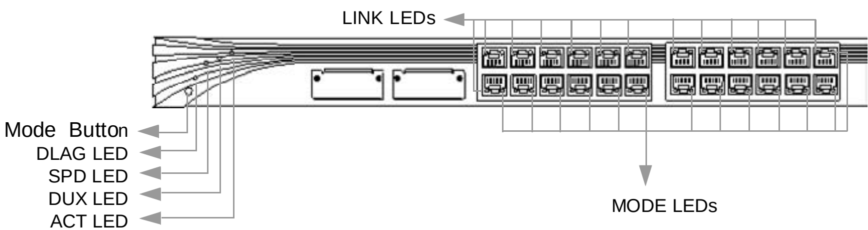


图 1-4 iSpirit /2924F **状态指示灯、模式键和端口** LED **状态指示灯位置图**

iSpirit 2924G **交换机百兆端口仅有一个** LED **指示灯，常亮表示** Link,**闪烁表示有数据。**iSpirit 2924F **交换机的每一个端口和** SFP **模块插槽都有两个** LED **状态指示灯，一个显端口或插槽的连接状态，一个显示端口的模式信息。表** 1-4 **说明端口** LED **连接状态指示灯的颜色及相应含义。**

表 1-4**：**

端口	颜色	状态
连接端口	无	无连接
	绿	连接

注 意 ：

SFP **模块和该端口号相同的** 10/100/1000Base-T **端口都正常连接网线的情况下，只有一个端口正常工作。所以只有一个端口的连接** LED **指示灯和模式** LED **指示灯正常显示端口的信息。**SFP **端口的优先级更高,即** SFP **模块连接到** SFP **插槽后，**SFP **插槽对应的** LED **灯正常显示该端口的信息。**

表 1-5 说明不同 ACT 模式下端口 LED 模式状态指示灯的颜色及相应含义。

表 1-5：

端口	颜色	状态
连接端口	无	无数据
	闪烁绿色	端口在发送或接收数据

1.5 交换机后面板说明

iSpirit 2924G/2924F 交换机后面板包含两个扩展模块插槽，一个电源接口，一个串口和一个风扇，一个堆叠开关。

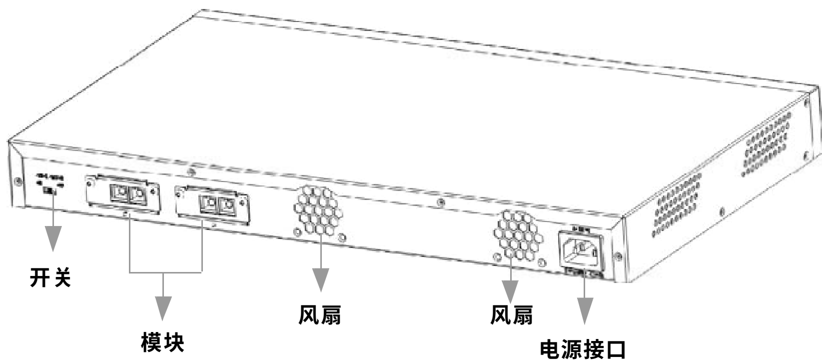


图 1-5A iSpirit 2924G 交换机后面板

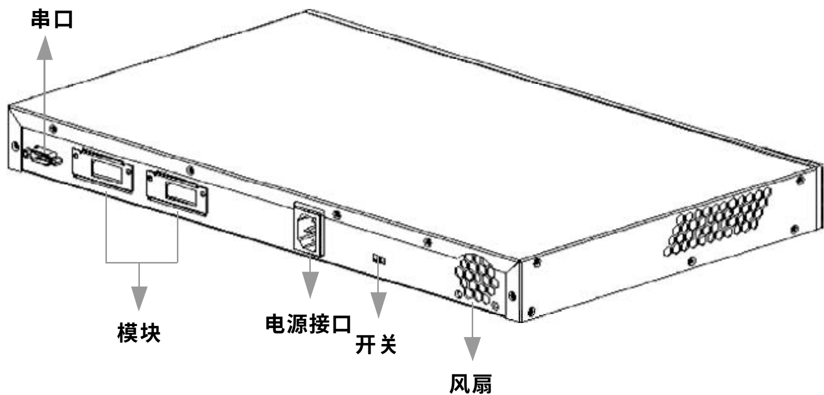


图 1-5B iSpirit 2924F 交换机后面板

1.5.1 电源接口

交换机支持从 180 伏到 240 伏的交流电压。使用时需要用交流电缆将电源接口与电源插座连接起来。

1.5.2 串口

用户可以通过使用 UART 串口和随机提供的专用控制端口电缆将交换机与一台 PC 机相连以实现对交换机的管理。控制端口电缆接插件的管脚配置参见附录 B。

第 2 章 交换机的安装与启动

本章主要说明如何正确安装并启动联想天工 iSpirit 2924G/2924F 交换机及如何上电自检测(POST)以确保交换机正常操作。用户需要仔细阅读以下内容并按顺序进行操作。

1、安装前指南
2、安装步骤
3、上电过程
4、连接步骤
5、Bootrom 启动选项介绍

2.1 准备安装

在安装之前,用户需要仔细阅读以下警告内容,对于任何因安装使用不当而造成的直接、间接、有意、无意的损坏及隐患，本公司概不负责。

警 告 ：

只允许经过培训有资格的技术人员安装或替换该设备。

在将设备与电源连接之前用户需要仔细阅读本用户手册。

在带电设备上工作之前，用户需要摘掉金属饰品（包括戒指、项链、手表等）。金属物品与电源和大地相连时会迅速升温，可能导致严重烧伤或将金属物品熔化在终端上。

不要将机箱放在其他设备上。如果机箱坠落可能造成严重的身体伤害或设备损害。

用户需要确保随时可以方便的关闭插座将设备断电。

为防止交换机温度过高，不要在超过建议的 45℃（113 ℉）环境温度下运行机器。为避免通风限制，在通风口前 7.6cm（3 英寸）处不放置杂物。

该设备在 TN 电源系统下正常工作。

当安装设备时，地线必须最先连接、最后断开。

该设备依赖建筑物的相应短路保护措施。注意在相导体上安装了保险丝或断路开关。

该设备需要接地。注意通常使用过程中要将主机接地。

将设备与电源相连时需要小心，防止线路超负荷。

电压不匹配可能造成设备损坏或火灾。如果设备标签上所示的电压与电源插座上的电压不相符，不要将设备与其相连。

交换机上如果没有开关，启动前需要断开电源线。

电源线未断开前不要接触电源。对于一个有电源开关的系统，当电源开关已关闭而电源线未断开时，电源内的线电压仍然存在。而对于一个没有电源开关的系统，在电源线未断开时，电源内的线电压也仍存在。

户外有闪电时不要在系统上工作或连接、断开网线。

该产品的最终处理符合国家的法律法规。

2.1.1 安装指南

交换机可以安装在桌面、机架、机柜或墙上。在安装之前首先需通过给交换机上电并运行 POST 以确认交换机工作正常。其步骤参见 “ 上电过程 ”。

警 告 ：

交换机里没有可用部件。如果用户拧开螺丝、打开机箱或拆开交换机都将使保修单无效。

1.安装位置指南

用户决定在何处安装该交换机时，请参照以下指南：

(1)从交换机 10/100Base-T 和 10/100/1000Base-T 端口到所连设备的最长距离不超过 140 米。

(2)从交换机 1000Base-X 端口到所连设备的最长距离不超过 10,000 米。

(3)布线需要远离电磁干扰，如收音机、电源线或荧光灯。

(4)交换机前后面板空间具体说明如下：

a.可以清晰看到前面板指示灯

b.可以方便地访问端口以使布线不受限制

c.电源线可以将后面板电源接口与 AC 电源插座相连

d.后面板通风孔附近 3 英寸空间内无杂物阻挡风流

(5)附录 A 中说明交换机的运行环境。

(6)交换机周围与通风口处的空气流通不受限制。

(7)交换机周围的温度不超过 40℃

注 意 ：

如果交换机安装在一个封闭的多层的机柜中其周围的温度会比正常温度高。

2.2 安装步骤

2.2.1 在桌面或机架上安装交换机

在桌面或机架上安装交换机时，请参考以下步骤：

(1)从安装包中拿出四个带胶条的橡胶垫。去掉橡胶垫上胶贴，将四个橡胶垫粘到交换机底部凹陷处。

(2)将交换机放到靠近 AC 电源的桌面或机架上。

(3)使用电源线将交换机与电源插座相连。连上电源以后，系统首先开始 POST 检测，这部分内容参考“上电过程”。

2.2.2 在机柜里安装交换机

警告：

为避免安装或使用机柜中交换机时造成身体伤害,用户必须采取有效的预防措施以确保交换机的稳固。请参阅以下指南以保证安全:

➲ 如果机柜内只有一台交换机，请把它安装到机柜底部。

➲ 如果机柜内有若干组件，请将其中组件按轻重顺序由上至下摆放。

➲ 如果机柜有固定装置，请先安装固定装置再安装交换机。

随交换机提供的机柜安装法兰可以安装在一个 19 英寸或 24 英寸的机柜上，其上安装孔参见图 2-1。

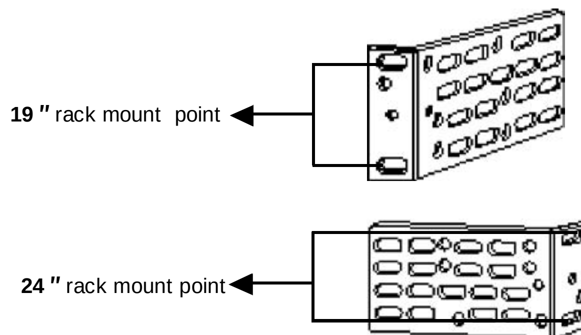


图 2-1 法兰安装孔

为了将交换机安装到一个 19 英寸或 24 英寸标准机柜中，需要参照以下步骤：

(1)从交换机上拧下螺丝

(2)将法兰安装在交换机上

(3)将交换机安装到机柜里

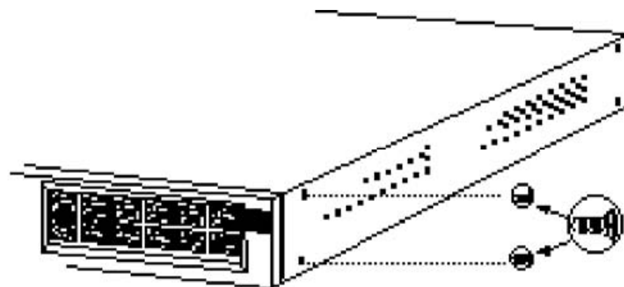


图 2-2 从交换机上拧下螺丝

1.将法兰安装在交换机上

法兰的方向及使用螺丝的选择需要根据用户选择的 19 英寸或 24 英寸的机柜而定。根据以下指南分别在每个法兰上安装两个螺丝。下面以 2924F 举例说明：

(1)对于 19 英寸机柜，用随机提供的螺丝将法兰的长边安装在交换机上。

(2)对于 24 英寸机柜，用随机提供的螺丝将法兰的短边安装在交换机上。

图 2-3、图 2-4 分别显示如何将法兰安装在交换机的前部和后部。在相反方向进行同样的安装。

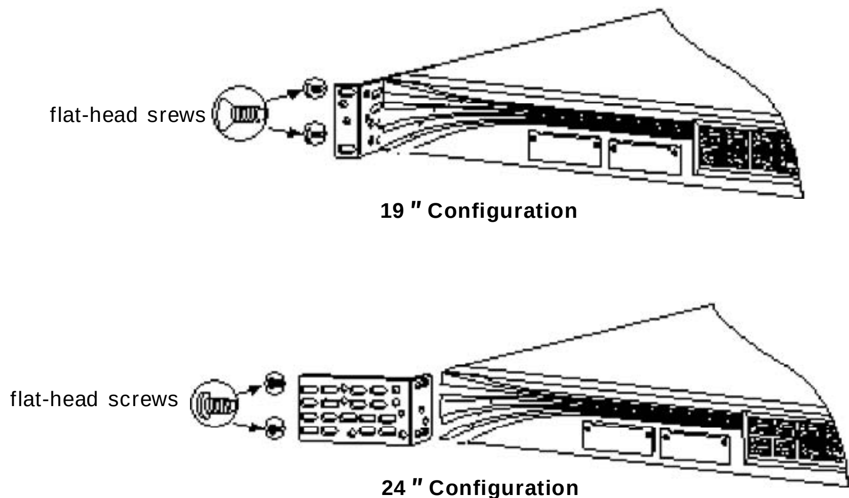


图 2-3 将法兰安装在交换机前部

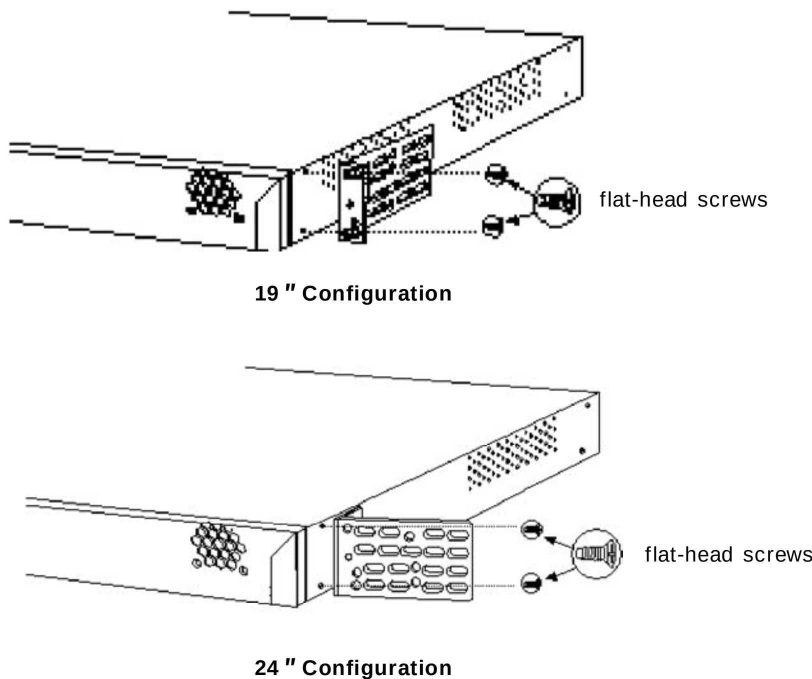


图 2-4 将法兰安装在交换机后部

2.将交换机安装到机柜里

把法兰安装在交换机上后，使用 4 个随机提供的螺丝将法兰安全固定在机柜里（如图 2-5 所示），然后把电源线插到交换机上。连上电源以后，系统首先开始 POST 检测。这部分内容参考“上电过程”。

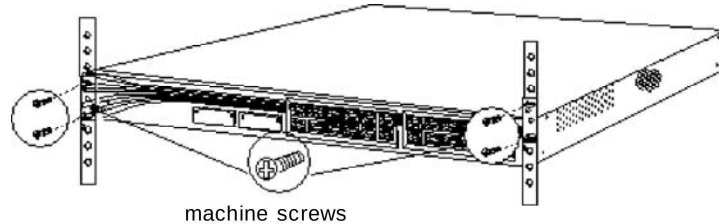


图 2-5 将 2924F 交换机安装到机柜里

2.2.3 在墙上安装交换机

为了把交换机安装到墙上，需要进行以下步骤：

(1)将法兰安装到交换机上

(2)将交换机安装到墙上

1.将法兰安装到交换机上

根据需要用户可以选择将交换机水平或垂直安装在墙上。

水平 / 垂直安装交换机：使用随机提供的螺丝将法兰的长边装在交换机上,将法兰的长边装在墙上,如图 2-6 所示。

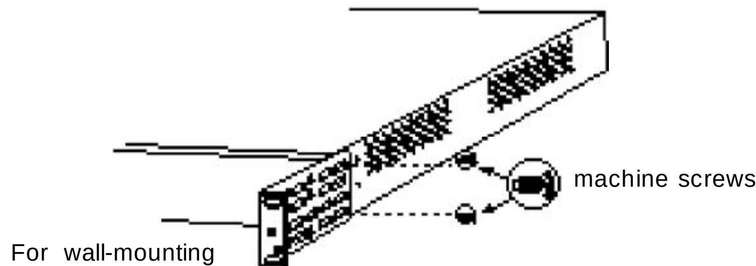


图 2-6 将法兰长边安装到交换机

2.将交换机安装到墙上

为了最好地支撑交换机及网线，用户需要确定将交换机安装在壁柱或安装板上（如图 2-7 所示），然后把电源线插到交换机上。下面以 2924F 举例说明：

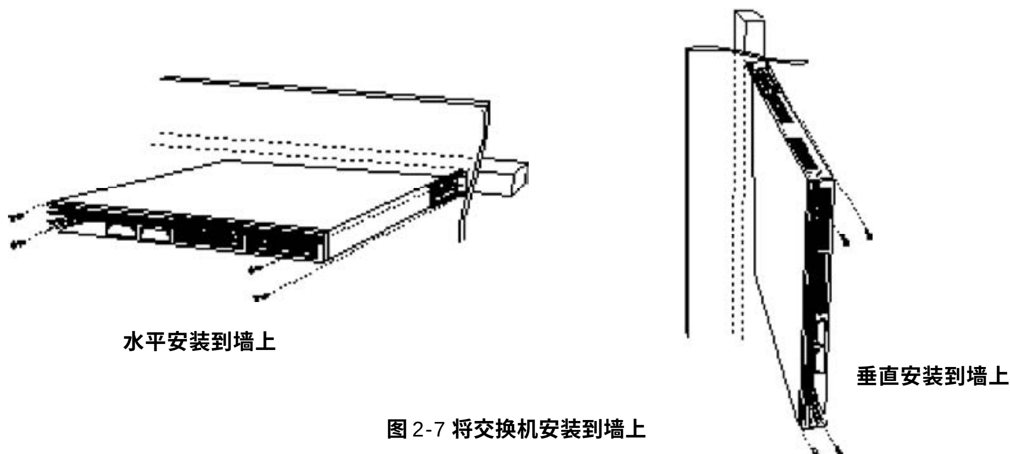


图 2-7 将交换机安装到墙上

2.3 上电过程

2.3.1 运行 POST 检测

安装好交换机后打开交换机需要进行以下步骤：

(1)电源线与交换机上的 AC 电源接口相连；

(2)电源线的另一端与 AC 电源插座相连。

交换机上电后前面板 28 个端口指示灯全部点亮，启动 BootRom 完毕后，全部熄灭。当交换机的二层功能启动开始时，点亮所有端口的指示灯，直到交换机启动完成后才熄灭。端口指示灯进入正常工作状态，在 ACT 模式下指示灯正常显示，表示交换机工作正常。

如果你的交换机不能通过 POST 检测，请立即通知交换机授权供应商。

2.4 连接步骤

以 iSpirit 2924G/2924F 交换机为例说明如何连接交换机。

2.4.1 连接交换机 10/100Mbps 端口

交换机 10/100Mbps 端口配置成以所连设备的速度运行。如果所连设备不支持自动协商，用户可以手工设定速度或双工模式等参数。根据以下步骤将交换机与 10Base-T 或 100Base-TX 设备相连，下面以 2924F 举例说明：

(1)对于 10Base-T 设备使用 CAT3、CAT4、CAT5 或 CAT5E 直连或交叉网线与交换机前面板的 RJ-45 端口相连。对于 100Base-TX 设备使用 CAT5 或 CAT5E 直连或交叉网线与交换机前面板的 RJ-45 端口相连（如图 2-8 所示）。网线的管脚说明参见附录 B 。

(2)将网线的另一端与所连设备的 RJ-45 端口相连。当交换机与所连设备建立连接之后，相应端口 LED 连接状态指示灯会亮。如果该灯不亮，可能是连接设备没开机，连接线路有问题或连接设备的网卡有问题。

(3)如果需要的话，重新配置并重启设备。

(4)重复 1 至 3 步以将每一个设备连接到 10/100Mpbs 端口。

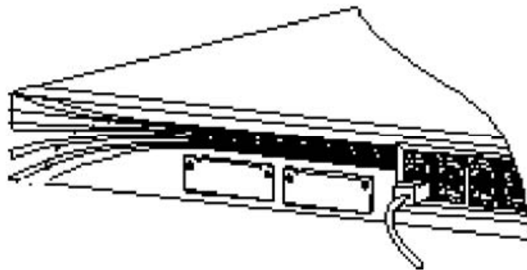


图 2-8 连接交换机 10/100Base-T 端口

2.4.2 连接交换机 100Base-X 或 1000Base-X 光纤模块端口

根据第一章描述内容将 100Base-X 光纤模块和 1000Base-X 光纤模块插入扩展模块插槽（不可热插拔）。

提示:

用户在没有准备好连接光纤前，请不要拔掉光纤端口的橡胶塞和光纤上的橡胶盖，以免光纤端口和光纤受到污染物或周围光线的损坏。

下面以 2924F 举例说明：

(1)当与工作站、服务器或路由器相连时使用 CAT5 或 CAT5E 直连网线与交换机前面板的 RJ-45 端口相连（如图 2-9 所示）。当与交换机或中继器相连时使用 CAT5 或 CAT5E 交叉网线。网线的管脚说明参见附录。

(2)将网线的另一端与所连设备的 RJ-45 端口相连。当交换机与所连设备建立连接之后，相应端口 LED 连接状态指示灯会亮。如果该指示灯不亮，可能是连接设备没开机，连接线路有问题或连接设备的网卡有问题。

(3)如果需要的话，重新配置并重启设备。

(4)重复 1 至 3 步以将每一个设备连接到 10/100/1000Base-T 端口。

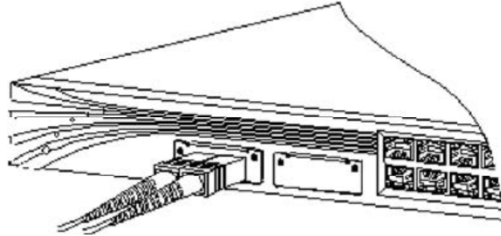


图 2-9 将 SC 接口插入光纤端口

2.4.3 连接交换机控制端口

使用随机提供的专用控制端口电缆将一台 PC 机或终端与交换机控制端口相连。控制端口和专用电缆的管脚信息参见附录 B。

PC 机或终端必须支持 VT100 终端模拟。终端模拟软件（如 PC 机应用软件 Hyperterminal 等）会在启动程序时建立交换机与 PC 机或终端间的通信。根据以下步骤将 PC 机或终端连接到交换机上：

(1)将随机提供的专用控制端口电缆插入交换机 UART 控制端口如图 2-10 所示。该电缆的管脚信息参见附录 B。

(2)将控制端口电缆的另一端插到所用 PC 的 UART 串口上。

(3)如果用户在使用 PC 机或终端，请启动终端模拟程序（超级终端 Hyperterminal）

(4)配置 PC 机或终端的字符格式，使其与交换机控制端口的以下缺省配置一致。

波特率：38400
数据位：8
停止位：1
校 验 ：无

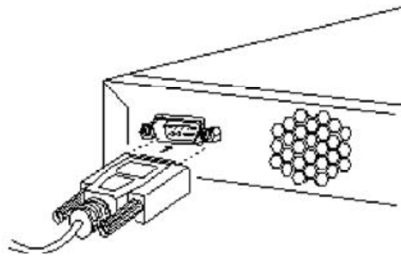


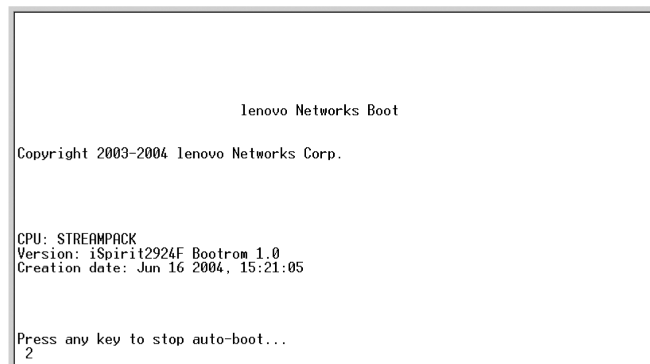
图 2-10 与 2924F 交换机控制端口连接

2.5 Bootrom 启动选项介绍

当交换机上电后，系统进入 Bootrom 启动过程。Bootrom 启动分为两种方式：自动启动和人工干预启动。

2.5.1 自动启动

在默认方式下，交换机在上电之后，如果用户不干预，交换机等待 3 秒后直接进入自动启动模式，开始启动映像程序。下面以 2924F 举例说明，在等待进入启动模式时的界面如图 2-11



```
lenovo Networks Boot

Copyright 2003-2004 lenovo Networks Corp.

CPU: STREAMPACK
Version: iSpirit2924F Bootrom 1.0
Creation date: Jun 16 2004, 15:21:05

Press any key to stop auto-boot...
 2
```

图 2-11 自动启动模式界面

2.5.2 人工干预启动

在等待进入启动模式的界面下输入除‘@’的任何键后进入 Bootrom 菜单界面，菜单提示符为“[Switch Boot]:”。在该提示符下，支持一些可用的命令，可以输入“？”显示帮助信息，下面以 2924F 举例说明，帮助信息如图 2-12。

```
                    lenovo Networks Boot

Copyright 2003-2004 lenovo Networks Corp.



CPU: STREAMPACK
Version: iSpirit2924F Bootrom 1.0
Creation date: Jun 16 2004, 15:21:05



Press any key to stop auto-boot...
 2
[Switch Boot]: _
```

图 2-12 人工干预启动模式界面

命令的功能

?	：显示帮助信息
@	：启动映像程序
b[<n>]	：显示或改变被激活的模式
p	：显示启动参数
c	：设置启动参数
P	：显示所有 PCI 设备

2.5.3 通过串口升级 hyper OS

在[Switch Boot]:下输入大写 D 出现§后，在超级终端的菜单选择传送，下面以 2924F 举例说明，如图 2-13 所示。协议选择 1K XModem，再选择发送即可。

注意：升级时请选用正确的升级文件。

```
                    lenovo Networks Boot

Copyright 2003-2004 lenovo Networks Corp.

        发送文件
        文件夹:   C:\Documents and Settings\yintt
        文件名(F):
        E\bootrom\bootrom.bin          浏览(B)...
CPU: STREAMPACK
Version: iSpirit2924F Boo     协议(P):
Creation date: Jun 16 200     1K Xmodem

                              发送(S)  关闭(C)  取消


Press any key to stop auto-boot...
 2
[Switch Boot]: D
serial loading............
Warning -- Target File Exists and is Being Overwritten
Ready to RECEIVE File /tffs/lenovo.Z in binary mode
Send several Control-X characters to cancel
§§§§§§§§§§§§§§§§§§§§§§§_
```

图 2-13 通过串口升级 hyper OS

2.6 下一步工作

用户可以通后面的章节介绍进一步配置和管理交换机。

第二部份 软件操作

第 1 章 产品综述

本章对 CLI 命令行接口进行详细的描述，主要包括以下内容：

1、模式介绍

2、命令语法介绍

3、行编辑

4、历史命令

1.1 CLI 命令行介绍

模式介绍

iSpirit2924G/2924F 交换机的 CLI 命令行接口包括很多的模式，不同的模式下包括不同的命令，可以对交换机执行不同的操作，下面对每一个模式进行介绍。

EXEC 模式

串口和 TELNET 首先进入的模式，进入此模式不需要输入口令。此模式的提示符是“Switch>”。该模式只有很少的几个命令可用，不能对交换机进行配置。在 EXEC 模式下输入 enable 命令并提供正确的口令即可进入全局配置模式。

全局配置模式

管理员才能进入的模式，进入该模式的用户可以完全控制交换机和浏览交换机的状态信息，并且可以对交换机进行配置。该模式有很多命令供用户使用。在全局配置模式下出现以下命令提示符：“Switch#”。

VLAN配置模式

在全局配置模式下执行命令 vlan <vlanid>进入 VLAN 配置模式,VLAN 配置模式是一个配置子模式，专门用于配置一个特定的 VLAN 的模式。VLAN 模式的提示符：“Switch(vlan-1)#”(vlan id 为 1 时)。

PORT RANGE配置模式

在全局配置模式下执行命令 port <p1-p2>进入 PORT RANGE 配置模式，PORT RANGE 配置模式是一个配置子模式，专门用于配置一个或多个连续的端口的模式。PORT RANGE 配置模式的提示符是：“Switch(port 1)#”（当端口是 1 时）或“Switch(port 1-4)#”（当端口是从 1 到 4 时）。

私有VLAN配置模式

在全局配置模式下执行命令 privatevlan <group-id>进入私有 VLAN 配置模式，该模式是配置子模式，配置一个私有 VLAN 组内的 VLAN 和端口配置信息,私有 VLAN 配置模式的提示符是：“Switch(privatevlan-10)#”（当私有 VLAN 组 ID 是 10 时)。

协议分类定义配置模式

在全局配置模式下执行命令 protocol definition <protocol classid>进入协议分类定义配置模式，该模式是配置子模式，配置一个协议分类定义的配置模式的提示符是：“Switch(protocol-10)#”（当协议分类 ID 是 10 时）。

1.2 命令语法介绍

命令组成

CLI 命令由关键字和参数两部分组成，一个关键字就是一个单词，可以有一个或多个，参数可以没有，也可以有一个或多个。如命令 save 就只有一个关键字而没有参数；命令 show switch 有两个关键字而没有参数；命令 vlan <vlanid>有一个关键字并且有一个参数；命令 ip address <ip-address> <subnet-mask>有两个关键字和两个参数。

参数类型

CLI 命令的参数分为两种：必选参数和可选参数。在输入命令时必选参数必须输入，而可选参数可以输入也可以不输入在命令语法中必选参数用< >表示，而可选参数用[ ]表示。

命令缩写

用户在 CLI 界面上输入命令时，命令的关键字可以缩写。CLI 支持命令的前缀匹配功能，只要输入的词与关键字前缀唯一匹配，CLI 就把输入的词解析成匹配的关键字。这样用户在使用 CLI 时非常方便，用户可以键入很少的的键完成一个命令，例如“show switch” 命令可以只键入“sh sw”。

语法帮助

CLI 命令行接口中设置有语法帮助，支持每一级命令和参数的帮助功能。如果您对某个命令的语法不太确定，请输入该命令中您所知道的前面的部分，然后键入“ ? ”，系统会提示您下一个命令的信息。您就可以根据提示的命令继续输入命令，直至提示命令为<cr>时，表明命令输入完毕。按回车执行所键入的命令。例如:“show ?”显示所有 show 命令的第二个关键词的帮助如“ip adrress 198.168.80.1 ?”能够询问下一个参数的含义。

1.3 行编辑

CLI 命令行接口支持行编辑快捷键功能，行编辑快捷键可以方便 CLI 命令的输入和编辑。用户在输入或编辑命令时，可以使用行编辑快捷键加速命令的输入。下面列出所有的行编辑快捷键及实现的功能：

Ctrl+c	中断
Ctrl+p 或↑键	上一条命令
Ctrl+n 或↓键	下一条命令
Ctrl+u	删除整行
Ctrl+a	光标回到行首
Ctrl+f 或→键	光标向右移动一格
Ctrl+b 或←键	光标向左移动一格
Ctrl+d	删除光标所在的字符
Ctrl+h	删除光标前一个字符
Ctrl+k	删除光标处及光标后的所有字符
Ctrl+x	删除光标处及光标前的所有字符
Ctrl+e	光标移到行尾

1.4 历史命令

CLI 命令行接口支持命令的历史记录功能，能记住用户最近使用的 20 个历史命令，把用户最近键入的命令保存起来。您可以用 show history 来显示已经输入过的命令，您也可以用 CTRL+P,CTRL+N 或上下键来选择历史命令。历史命令功能可以方便用户输入命令。

第 2 章 配置通用功能

在 iSpirit 2924G/2924F 交换机中，有一些功能很简单，但很常用，一并在本章中介绍，主要包括以下内容：

1、系统基本配置

2、配置文件管理

3、软件版本升级

2.1 系统基本配置

用户可以在全局配置模式（Switch#）下使用 CLI 命令，这些命令用于维护交换机的通常管理，比如修改密码、显示交换机配置信息等。

首先在 EXEC 模式，执行 enable 指令，输入密码后进入全局配置模式，如下所示：

Switch> enable
Password：
Switch#

- **设置交换机的 VLAN1 的 IP 地址及子网掩码**

  ip address <ip-address><subnet-mask>

  例： Switch# ip address 192.168.2.3 255.255.255.0

- **设置交换机的缺省网关**

  ip gateway <gateway-address>

  例：Switch# ip gateway 192.168.2.1

- **重新启动计算机**

  Switch# reset

- **重新启动计算机，并恢复到出厂模式**

  Switch# reset factory

- **修改交换机口令，交互式命令，新设的口令需要输入两次**

  Switch# password

  注：交换机缺省 Password 是空。

- **把配置信息保存在 flash 中**

  Switch# save

- **回到上一级模式，如果目前处于全局配置模式，回到 EXEC 模式，如果目前处于 EXEC 模式，执行的命令与 logout 一样。**

  Switch# exit

- **适用于任何 CLI 模式，退出 TELNET 终端，对串口的终端无效**

  Switch# logout

- **清除屏幕上的所有信息**

  Switch# cls

- **测试交换机与远端机器的网络连通性**

  Switch# ping <remote-host>

  例：假设交换机的 IP 地址是 198.168.80.1，有一台直连主机的 IP 地址是 198.168.80.72，交换机测试主机的连通性。

  Switch# ping 198.168.80.72

  连通显示：

  PING 198.168.80.72: 56 data bytes
  64 bytes from host (198.168.80.72): icmp_seq=0. time=0. ms
  64 bytes from host (198.168.80.72): icmp_seq=1. time=0. ms
  64 bytes from host (198.168.80.72): icmp_seq=2. time=0. ms
  64 bytes from host (198.168.80.72): icmp_seq=3. time=0. ms
  64 bytes from host (198.168.80.72): icmp_seq=4. time=0. ms
  — — 198.168.80.72 PING Statistics— —
  5 packets transmitted, 5 packets received, 0% packet loss
  round-trip (ms) min/avg/max = 0/3/16

  未连通显示：

  PING 199.168.80.72: 56 data bytes
  no answer from 199.168.80.72

- **显示最近 20 条历史指令**

  Switch# show history

- 显示交换机的系统信息。系统描述、产品名称、版本信息、启动时间等
  Switch# show system
- 显示交换机的一些配置信息。IP 地址、MAC、IP gateway 和协议的启用情况
  Switch# show switch
- 显示串口连接参数
  Switch# show console
- 显示当前会话的终端的宽度和高度（能显示多少个字符）
  Switch# show terminal
- 显示交换机的 VLAN1 的 IP 地址信息。IP 地址，子网掩码、网关
  Switch# show ip
- 显示交换机的版本信息
  Switch# version
- 设置 TELNET 的登陆密码，
  Switch# set telnet password
  注：TELNET 的缺省密码为 123。
- 清除 TELNET 的登录密码
  Switch# clear telnet password
- 配置 CLI 自动退出的时间
  Switch# idletime <timeout>
- 显示 CLI 自动退出的时间
  Switch# show idletime
- 配置系统时间
  Switch# set time
- 配置系统提示符
  Switch# switchname <switch-name>

2.2 配置文件管理

当用户修改了交换机的配置后，最好把配置信息存储在 FLASH 中，这样交换机重新启动后配置依然存在。管理员也可以通过 TFTP 完成配置文件的上传和下载。

命令

在 CLI 各种模式下都可以执行存储操作：

save

在全局配置模式下，可以将交换机的配置文件进行备份，上传到指定的主机上：

upload configuration <ip-address> <name>

ip-address：表示文件上传的目的 PC 的 IP 地址。

name：表示配置文件的命名。

在全局配置模式下，可以把指定的主机上的配置文件下载到交换机上：

download configuration <ip-address> <name>

ip-address：表示文件下载的 PC 的 IP 地址。

name：表示下载的文件的文件名。

要想下载的配置能够生效，必须重启交换机。

2.3 上传和下载配置

操作步骤如下：

第一步：搭建备份文件需要网络环境

第二步：将交换机配置信息生成配置文件；

第三步：将配置文件备份到 PC（备份过程已经完成，必要时，进行下一步操作）

第四步：将配置的备份文件重新下载到交换机。

示例：一台已经配置了 vlan 和接口地址的交换机，需要进行配置文件备份。

第一步：搭建如下所示网络环境

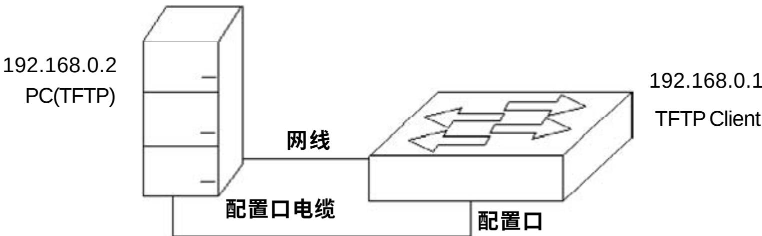


图 2-1 网络环境图

将交换机的配置口通过电缆外接一台配置终端，并通过网线与一台 PC 相连。在 PC 安装 TFTP Server，配置 PC 的以太网口 IP 地址，这里假定 PC 的 IP 地址为 192.168.0.2。然后，配置交换机以太网口 IP 地址，这里假定交换机的 IP 地址为 192.168.0.1。

注 意 ：

PC 网口 IP 地址与交换机以太网口 IP 地址应位于同一网段。

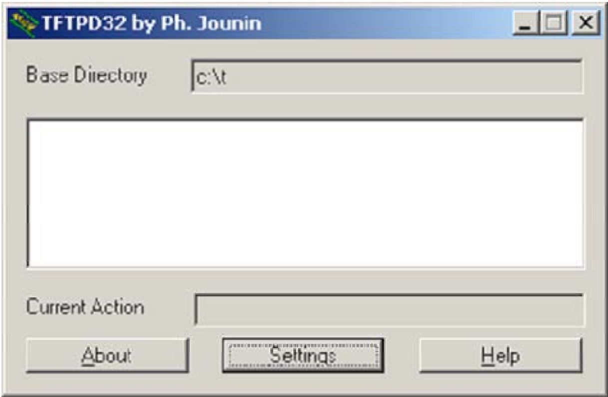


图 2-2 TFTPD32 界面图

然后，设置备份配置文件的目录。具体操作是，单击[Settings]按钮，出现 TFTPD32 设置界面，如下图。

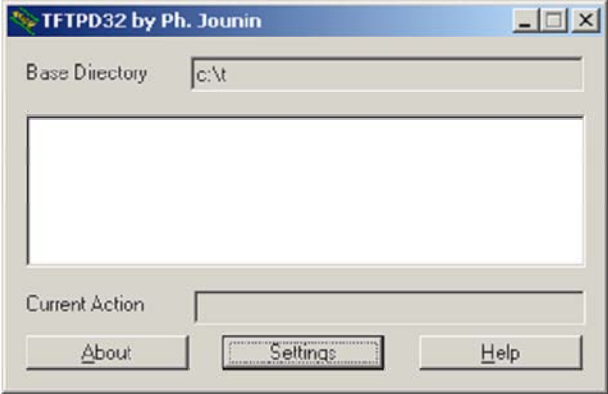


图 2-3 TFTPD32 设置界面图

在“Base Directory”中输入文件路径。单击[OK]按钮确认。

第二步：将交换机的配置信息生成配置文件

在交换机任意管理模式下执行 save 指令，就可以将配置信息生成配置文件。

第三步：将文件备份到 PC 上

Switch# upload configuration 192.168.0.2 beifen
uploading configuration ......
complete
Switch#

第四步：必要时，将备份文件下载到交换机

Switch# download configuration 192.168.0.2 beifen
Do you wish to continue? [Y/N]: y
downloading configuration ......
Complete.

第五步：要想下载的配置文件能够生效，必须重启交换机

Switch# reset

Do you wish to continue？**是询问操作是否继续进行。Y 表示是；N 表示否。**

2.3.1 上传配置实例

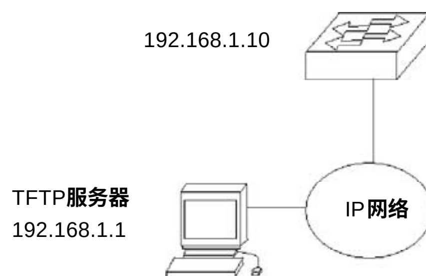


图 2-3 上传配置需求

把交换机的配置文件上传到 TFTP 服务器上

TFTP **服务器的** IP **地址为** 192.168.1.1 2924G/2924F **交换机的** IP **地址为** 192.168.1.10,**首先** TFTP **和交换机的** IP **之间能够相通。**

在TFTP上打开TFTP服务

在交换机上执行

Switch# upload configuration 192.168.1.1 **文件名**
uploading configuration ......

把 TFTP 服务器上的配置文件向下传到交换机上

Switch# download configuration 192.168.1.1 **文件名**
Do you wish to continue? [Y/N]: y

排错：

如果上传不成功，需要注意以下几个方面：

1、tftp **服务器和交换机之间的** IP **是一定要相互能通**
2、tftp **服务器的** tftp **服务一定要打开**
3、**在交换机上执行的上传配置文件的命令一定要写正确**

如果把配置文件从 tftp **服务器上下传到交换机上不成功，需要注意以下几个方面：**

1、tftp **服务器和交换机之间的** IP **是一定要相互能通**
2、tftp **服务器的** tftp **服务一定要打开**
3、**在交换机上执行的下传配置文件的命令一定要写正确，特别是配置文件的名字一定要正确，区分大小写。**

4、准备好的配置文件一定要放置到 tftp 服务器指定的目录下

2.4 软件版本升级

iSpirit2924G/2924F 交换机软件版本支持在线升级。升级是通过工具 TFTP 来完成的。

命令

在全局配置模式下，可以将交换机的映像文件升级：

download image <ip-address> <name>

其中<ip-address>为 PC 机的 IP 地址,<file-name>为在 PC 机上映像程序文件名。在下载的过程中不能断电，否则交换机的映像文件可能损坏而造成交换机启动不了。下载完毕后，需要重新启动交换机才能运行新下载的映像文件程序。

软件升级过程

升级映像文件步骤：

1、搭建升级环境

第一步：搭建升级环境。如下图所示。

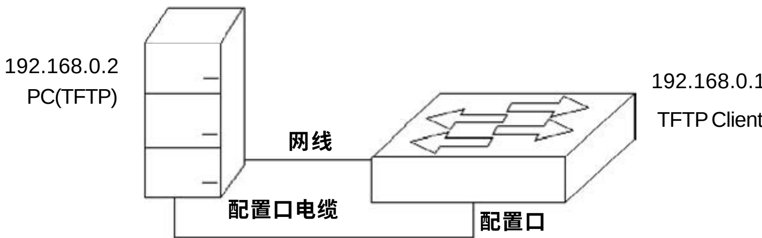


图 2-4 搭建 TFTP 升级环境

第二步：将交换机的配置口通过电缆外接一台配置终端；

第三步：在微机上安装 TFTP Server；

第四步：将新的映像文件拷贝到某一路径下，这里假定路径为 C:\t；

第五步：配置微机的以太网口 IP 地址，这里假定微机的 IP 地址为 192.168.0.2；

第六步：配置交换机以太网口 IP 地址，这里假定交换机的 IP 地址为 192.168.0.1。

注 意 ：

主机网口 IP 地址与交换机以太网口 IP 地址应位于同一网段。

2、运行 TFTP Server

第一步：运行 TFTP Server。TFTPD32 窗口界面如下图：

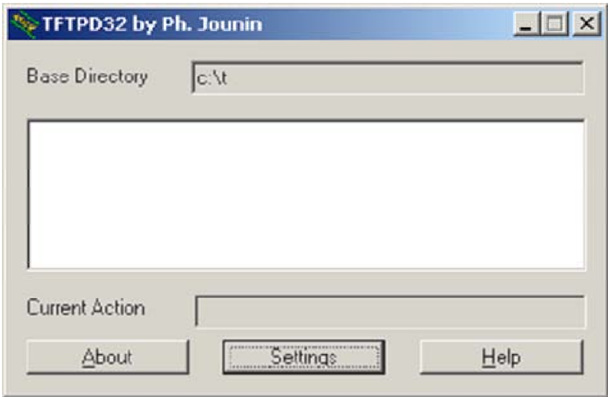


图 2-5 TFTPD32 界面图

第二步：设置 TFTP Server 文件目录。启动 TFTP Server 之后，重新设置 TFTP Server 文件目录，将待加载的映像文件拷贝到此目录之中。具体操作是，单击[Settings]按钮，出现 TFTPD32 设置界面，如下图。

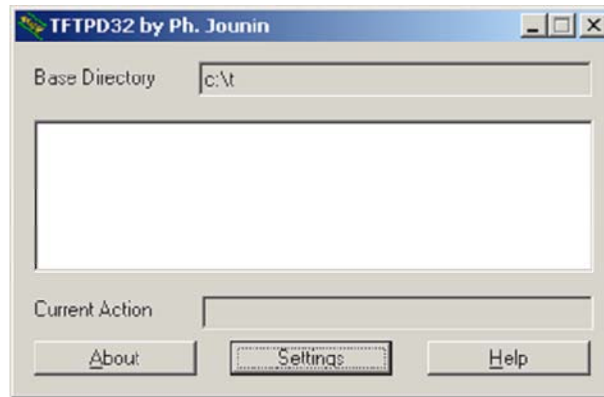


图 2-6 TFTPD32 设置界面图

在"Base Directory"中输入文件路径。单击[OK]按钮确认。

3. **配置交换机**

第一步：连接交换机，选择以太网接口后，将该接口与运行 TFTP Server 程序的主机通过以太网线连接。并用 ping 命令检测主机与交换机之间是否连通。

第二步：在超级终端 Switch# 中输入命令：

Switch# download image 192.168.0.2 lenovo.img，**回车，等待下载映像文件完毕。**

Do you wish to continue? [Y/N]: y

downloading image......

Complete.

Switch#

注意：交换机升级过程中，不能断电，且时间段长，请耐心等待。

第三步：重新启动交换机。

Switch# reset

2.4.1 升级实例

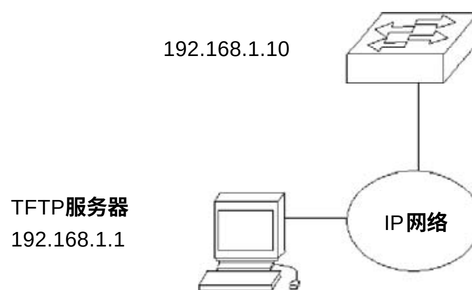


图 2-7 升级配置实例

从 TFTP 服务器上升级交换机的映像文件

TFTP **服务器的** IP **地址为** 192.168.1.1 2924G/2924F **交换机的** IP **地址为** 192.168.1.10,**首先** TFTP **和交换机的** IP **之间能够相通，映像文件名为** 2924G/2924F.img

在 TFTP 上打开 TFTP 服务，并且把要升级的交换机映像文件放 TFTP 服务器上指定的目录下，然后在交换机上执行。

```
Switch# download image 192.168.1.1 2924G/2924F.img
 Do you wish to continue? [Y/N]: y
 Don't Shut down power until completed!
 downloading image ......
```

一直等到交换机提示升级完成，然后才能重新启动交换机

排 错 ：

交换机映像文件升级不成功，需要查找以下几个原因：

1、**交换机和** TFTP **服务器之间是否** IP **能够通信**

2、TFTP **服务器是否正常启动，并且启动所用的** IP **地址就是交换机所能够** PING **通的**

3、**映像文件是否放到了** TFTP **服务器所指定的特定位置**

4、**在交换机上执行升级映像文件时，映像文件的名字一定不要写错。**

第 3 章 配置端口

本章对端口相关的配置进行介绍，主要包括以下内容：

1、**流控**

2、**端口限速**

3、**广播抑制**

4、arl **配置**

5、mirror

6、trunk **配置**

7、MAC **地址过滤配置**

8、**端口锁定**

3.1 流控

- **开启流控命令：**flow-control ports A-B or A (port list 1<=A,B<=28)**，开启端口**3、4**的流控功能配置事例如下：**
  switch# flow-control ports 3-4
- **关闭流控命令：**no flow-control ports A-B or A (port list 1<=A,B<=28)**，关闭端口**3、4**的流控功能配置事例如下：**
  switch# no flow-control ports 3-4
- **察看流控状态流控命令：无单独的流控状态查询命令，作为端口状态的一种属性，可通过查询端口状态间接获取（参见端口状态查询命令）。**

3.2 端口限速

- **端口限速开启命令：进入到端口配置模式，**bandwidth limit**，输入该命令后进入端口限速配置状态，根据提示即可完成限速配置。（端口限速方式可配置为单向接收限速、单向发送限速、双向限速，限速粒度为**64 kbytes **）。限制端口**2**接收带宽为**64KB**，发送带宽为**128KB**的配置事例如下：**
  switch#port 2
  switch(port(1-2))#bandwidth limit
  Bandwidth type (1-Rx 2-Tx 3-Rx/Tx):3
  Rx bandwidth value (64-12800)k bytes:64
  Tx bandwidth value (64-12800)k bytes:128
  Switch(port(1-2))#
- **端口限速关闭命令：进入到端口配置模式，**no bandwidth limit**。关闭端口**2**的限速功能的配置事例如下：**
  switch#port 2
  switch(port(1-2))#no bandwidth limit
  switch(port(1-2))#
- **察看当前端口限速状态命令：在端口配置模式下，**
  show bandwidth。

端口限速配置实例

端口限速方式可配置为单向接收限速、单向发送限速、双向限速，限速粒度为64 kbytes。
限制端口2**接收带宽为**64KB**，发送带宽为**128KB**的配置事例如下：**
switch#port 2
Switch(port(2-2))#bandwidth limit
Bandwidth type (1-Rx 2-Tx 3-Rx/Tx):3
Rx bandwidth value (64-12800)k bytes:64
Tx bandwidth value (64-12800)k bytes:128
Switch(port(2-2))#
端口限速关闭命令：进入到端口配置模式，no bandwidth limit**。关闭端口**2**的限速功能的配置事例如下：**
switch#port 2
Switch(port(2-2))#no bandwidth limit
Switch(port(2-2))#
察看当前端口限速状态命令：在端口配置模式下，
show bandwidth。

Port	Flag	RxBand	TxBand
1	disable	——— KB	——— KB
2	Rx/Tx	64 KB	128 KB

3.3 广播抑制

- **广播抑制配置命令：**storm-control,**输入该命令后进入端口广播抑制配置状态，根据配置提示即可完成广**

播抑制的配置。开启端口 1-4 广播抑制功能，限制广播所占用带宽为 0-1250000 bytes/秒，配置事例如下：

```
switch#storm-control
    Enable storm control(y/n) :y
    Enable storm control ports list : 1-4
    Port broadcast flow rate range(0-1250000 bytes) :10000
Switch#
```

关闭端口 1 － 4 广播抑制功能的配置事例如下：

```
    switch#storm-control
    Enable storm control(y/n) :n
    Disable storm control ports list : 1-4
Switch#
```

➢ 察看当前广播抑制配置状态命令：show storm-control。

3.4 ARL 配置

Address Resolution Logic 的简称，是二层交换机硬件转发数据帧的核心。硬件根据数据帧的目的 MAC 地址查找 ARL 表找到相应的表项，并把数据帧送到相应的输出端口。交换机根据数据帧的源 MAC 地址以及发送端口自动学习生成表项。除自动学习外，管理员也能定制 ARL 表项。ARL 命令就是用于管理 ARL 表的命令。

增加或删除一个单播或组播表项

➢ 命令：arl
模式：CONFIGURATION
功能：向 ARL 表中加入一个表项，包括单播 MAC 地址表项和多播地址表项。此命令是一个交互输入的命令，命令执行后首先要用户输入 MAC 地址，命令再根据 MAC 地址是单播地址还是多播地址提示用户输入不同的信息。对于单播地址，还需要输入 MAC 地址对应的端口号以及此表项是静态的还是动态的。对于多播地址，还需要输入端口链（即可以输入多个端口），VLAN ID 以及该表项是静态的还是动态的。

➢ 命令：no arl <mac-address>
模式：CONFIGURATION
功能：从 ARL 表中删除给定的单播 MAC 地址的表项。

➢ 命令：no marl <mac-address>
模式：CONFIGURATION
功能：从 ARL 表中删除给定的多播 MAC 地址表项。

显示 arl 信息

➢ 命令：show arl all
模式：CONFIGURATION
功能：显示 ARL 表中的所有单播地址表项。

➢ 命令：show marl all
模式：CONFIGURATION
功能：显示 ARL 表中的所有多播地址表项。

➢ 命令：show arl ports <port-list1> [<port-list2>] ...... [<port-listn>]
模式：CONFIGURAITON
功能：显示 ARL 表中所有给定端口的单播地址表项。

➢ 命令：show arl mac <mac-address>
模式：CONFIGURATION
功能：显示 ARL 表中 MAC 地址与给定 MAC 地址相同的表项，包括单播地址表项和多播地址表项。

➢ 命令：show arl age-interval
模式：CONFIGURAITON
功能：显示二层交换表表项超时时间

➢ 命令：arl age-interval <age>

模式：CONFIGURAITON
功能：设置表项超时时间

3.5 mirror

交换机端口镜像功能就是用户将所有的流量从一个特定的端口复制到一个指定的镜像端口，以便进行流量分析和协议分析。这样，这些流量就可以被一个特殊的设备监控。它对发现和解决故障有很大的帮助。]

联想天工 iSpirit 2924G/2924F 交换机能够分别侦听端口的进入数据和出去的数据。一个侦听端口只能侦听一个端口，而且只能有一对侦听端口和被侦听端口，同时，侦听端口只能监测被侦听端口的数据，不能和交换机通讯 。

例如：端口 1 设为侦听端口，侦听端口 2 的数据，那么端口 1 所连接的 PC 就不能 ping 通交换机。

- **命令：**mirror
  模式：CONFIGURATION
  功能：创建一个 mirror
  Switch# mirror

示例：通过镜像，使端口 3 **侦听端口** 2 **流出的流量。**

Source Mirror Port (1-28) : 2
Destilation Mirror Port(1-28): 3
Mirror mode select (Rx/Tx) : rx

说明： Destilation Mirror Port 为镜像端口,Tx 表示侦听流出的数据，Rx 表示侦听流入的数据。只能设置一个侦听端口和被侦听端口。

- **命令：**no mirror
  模式：CONFIGURATION
  功能：删除 mirror **设置**
  Switch# no mirror
- **命令：**show mirror
  模式：CONFIGURATION
  功能：查看交换机的 mirror **设置**
  Switch# show mirror

3.5.1 mirror实例



图 3-1 端口镜像配置

在一台交换机中，用户 1 和用户 2 正在通信，正常情况下其他端口的用户是无法获取其通信信息的，为了检测数据流是否正常，监测者需要获取其数据流，就要用到端口镜像问题 。用户 1 连接到端口 1，用户 2 连接到端口 2，监测者连接在端口 8，使监测者能够捕捉到其数据流。

通过监测用户 1 的流量

Switch# mirror
Source Mirror Port (1-28) : 1
Destilation Mirror Port(1-28) : 8
Mirror mode select (Rx/Tx) : tx

也可以通过监测用户 2 的流量

Switch# mirror
Source Mirror Port (1-26) : 2
Destilation Mirror Port(1-26): 8
Mirror mode select (Rx/Tx) : tx
排 错 ：
show mirror **命令进行确认**
Switch# show mirror
Mirror function enable.
Current mirror mode : Tx.
Source mirror port : 1
Destination mirror port: 8
确保镜像配置正确

3.6 Trunk 功能配置和管理过程

Port Trunking **技术是一种将网络流量聚集在一组端口上的方法，以形成一个交换机之间的大容量的通道或容错的通道。通道之间可以实现流量均衡。联想天工** iSpirit 2924G/2924F **交换机支持** Port Trunking**，通过创建** Port Trunking **来提升交换机之间的带宽。**Port Trunking **把多个物理端口捆绑在一起当作一个逻辑端口来使用。如果** Port Trunking **中的一个端口发生堵塞或故障，那么数据包会被重新分配到该** Port Trunking **中别的端口进行传输。如果这个故障端口重新恢复正常，那么数据包将重新分配到该** Port Trunking **中的所有端口进行传输。**

交换机的 trunk **功能配置分为以下几个步骤：**
第一步：创建 trunk **组**
第二步：修改 trunk **组的参数**

- **创建一个** port trunking **组**

  Switch # trunk
  在这个交互操作中一次输入 rtag<1-4>、tid<0-3>、port list
  注意：本产品支持 4 **个聚合。每个聚合支持八个** 10/100M **端口聚合在一起。这是一个交互式命令，首先输入** rtag **号，接着输入** trunk id **号，接端口聚合的方法它的值为** 1 － 4，1 **：基于源** MAC **地址；**2 **：基于目的的** MAC **地址；**3 **：基于源异或（**xor**）目的的** MAC **地址；**4 **：基于源与（**and**）目的的** MAC **地址。最后输入** trunk ports **列表。**
  示例：将 1 － 8 **端口设置到** tid **是** 1 **的** rtag **是** 2 **的** trunk **组**
  Switch # trunk
  Trunk_rtag:2
  Trunk_id:1
  Ports_list:1-8

- **取消** trunk **组**

  Switch# no trunk <tid>

- **显示** trunk **配置**

  Switch# show trunk

- **修改已经配置的** trunk **组的聚合方式**

  Switch# trunk rtag <tid> <rtag>

- **修改已经配置的** trunk **组的端口成员**

  Switch# trunk ports <tid> <port list>

- **删除已经配置的** trunk **组的成员**

  Switch# trunk no ports <tid> <port list>

3.6.1 Trunk 配置案例

配置交换机 1 **和交换机** 2 **之间做** trunk **链路，各自捆绑** 1-4 **端口做链路聚合在每个交换机上执行：**
Switch# trunk port 1 1-4 <cr> set trunk configuration
注意，做 trunk **时，两边交换机的端口数量要一致，速度、双工等端口参数都要完全一致，但不必两边的**

端口号一一对应

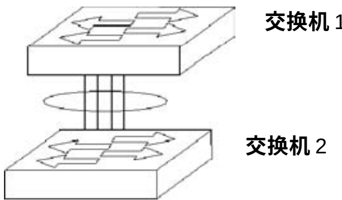


图 3-2 TRUNK 功能典型配置

删除一个 trunk 组

Switch# no trunk A   trunk indentifier(0<=tid<=3)

删除所有的 trunk 组

Switch# trunk table init <cr>

排错：

1、如果 trunk 没有起作用，需要查看以下状态

Switch# show trunk

TGID	RTAG	status	Ports
0	1	Not_ready	()
1	1	Active	(01 02 03 04)
2	1	Not_ready	()
3	1	Not_ready	()

检查所配置的 trunk 是否激活，包含的端口数量和端口号是否正确。

2、加入 trunk 组的几个端口一定要属于同一个 vlan，速率，双工等端口属性都要设置一样。

3.7 MAC 地址过滤配置

iSpirit 2924G/2924F **交换机可以根据报文的目的** mac **地址进行过滤。**

配置过程如下：

1、配置 MAC 地址过滤。

mac filter <vlanid> <mac address>

参数说明：

vlanId：mac **地址所在的** vlan。

mac-address：**要绑定的** mac **地址。**

配置示例：

Switch# mac filter 2 00:10:5c:af:ba:a9

2、删除 MAC 地址过滤配置。

no mac filter <vlanid> <mac address>

参数说明：

vlanId：mac **地址所在的** vlan。

mac-address：**要绑定的** mac **地址。**

配置示例：

Switch# no mac filter 2 00:10:5c:af:ba:a9

3、显示 MAC 地址过滤配置。

show mac filter

3.8 端口锁定

命令：lock ports <port-list1> [<port-list2>] ...... [<port-listn>]

模式：CONFIGURAITON

功能：锁定端口列表指定的端口，以禁止其学习 MAC **地址。**

命令：unlock ports <port-list1> [<port-list2>] ...... [<port-listn>]

模式：CONFIGURAITON

功能：解锁端口列表指定的端口，允许其学习 MAC **地址。**

第 4 章 VLAN 配置

本章主要包括以下内容：

1、VLAN **介绍**
2、VLAN **配置**
3、VLAN **配置示例**

VLAN 是交换机中的一个重要概念，在实际应用中使用非常多，它是内部划分多个网络的基础。VLAN 是虚拟局域网的简称，它是逻辑地把多个设备组织在一起的一个网络，它不管设备的物理位置在哪里。每个 VLAN 都是一个逻辑网络，它具有传统的物理网络的一切功能和属性。每个 VLAN 都是一个广播域，广播包只能在一个 VLAN 内进行广播，不能跨越 VLAN，VLAN 间的数据通信必须通过三层转发。

iSpirit 2924G/2924F 交换机中有 VLAN 和私有 VLAN、协议 VLAN、PVID 的概念，所以通常又把 VLAN 称为普通 VLAN，本章介绍普通 VLAN 和协议 VLAN、PVID 的配置，关于私有 VLAN 的配置请参见“配置私有 VLAN”章节。

本章主要包括以下内容：

- VLAN 介绍
- VLAN 配置
- VLAN 配置示例
- 协议 VLAN
- 保护 VLAN

4.1 VLAN 介绍

本节对 VLAN 进行一个详细的介绍，主要包括以下内容：

- VLAN 的优点
- VLAN ID
- VLAN 端口成员类型
- VLAN 中继
- 数据流在 VLAN 内的转发
- VLAN 与私有 VLAN 的关系
- 协议 VLAN 的配置
- 端口的 PVID 的配置
- 端口的 INGRESS FILTER 的 VLAN 属性的配置
- 端口的 acceptable frame-type 属性的配置
- 保护 VLAN 的配置

VLAN 的优点

VLAN 极大地扩展了物理网络的规模。传统的物理网络只能有一个很小的规模，最多能容纳上千台设备，而使用 VLAN 划分的物理网络能够容纳上万甚至几十万台设备。VLAN 与传统的物理网络有相同的功能和属性。

使用 VLAN 有以下好处：

1.VLAN 能有效控制网络中的流量

在传统网络中，不管有无必要，所有的广播包都传送到所有的设备，加重了网络和设备的负载。而 VLAN 能够根据需要把设备组织在一个逻辑网络中，一个 VLAN 就是一个广播域，广播包只在 VLAN 内部传送，不会跨越 VLAN。通过划分 VLAN 可以有效地控制网络中的流量。

2.VLAN 能够提高网络的安全性

VLAN 内的设备只能与同一个 VLAN 的设备进行二层通信，如果要与另一个 VLAN 通信，必须通过三层转发，如果不建立 VLAN 间的三层转发，VLAN 间完全不能通信，可以起到隔离的作用，保证每个 VLAN 内的数据安全。例如一个公司研发部不想与市场部的数据进行共享，可以研发部建立一个 VLAN，市场部建立一个 VLAN，二个 VLAN 间不建立三层通信通道。

3.VLAN 使设备的移动变得方便

传统的网络中的设备如果从一个位置移动到另一个位置而属于不同的网络时，需要修改移动设备的网络配置，这样对于用户来说是非常不方便的。而 VLAN 是一个逻辑网络，可以把不在同一物理位置的设备划在同一个网络，当设备移动时还可以使设备属于此 VLAN 中，这样移动的设备不需要修改任何配置。

VLAN ID

每一个 VLAN 有一个标识号，叫 VLAN ID，VLAN ID 的范围从 0 到 4095，其中 0 和 4095 不用，实际有效

的只有 1 到 4094。VLAN ID 唯一标识一个 VLAN。

在网络中的一个 VLAN 内传输的数据帧有三种：不带标记的数据帧，带 VID 为 0 的标记的数据帧，带 VID 非 0 的标记的数据帧。如图 4-1 所示为三种不同数据帧格式。

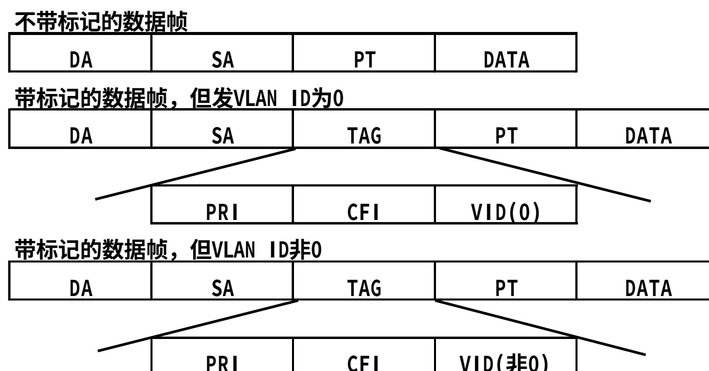


图 4-1 三种不同的数据帧格式

在交换机内部所有的数据帧都是带标记的。如果一个不带标记的数据帧输入交换机，交换机要给该数据帧加上一个标记，选择一个 VLAN ID 值填入标记的 VID 中。如果一个带 VID 为 0 的标记的数据帧输入交换机，交换机选择一个 VLAN ID 值填入标记的 VID 中。如果一个带 VID 非 0 的标记的数据帧输入交换机，该帧不变。

VLAN 端口成员类型

iSpirit 2924G/2924F 交换机支持基于端口的 VLAN 和基于 802.1Q 的 VLAN。一个 VLAN 包括两种端口成员类型：untagged 成员和 tagged 成员。一个 VLAN 可以既包括 untagged 端口成员，又包括 tagged 端口成员。

一个 VLAN 可以没有端口成员，也可以有一个或多个端口成员。当一个端口属于一个 VLAN 时，可以是 VLAN 的 untagged 成员或 tagged 成员。

一个端口最多只能属于一个 VLAN 的 untagged 成员，当一个端口设置成一个 VLAN 的 untagged 成员时，如果该端口还属于其它 VLAN 的 untagged 成员，则把该端口从其它 VLAN 中清除，也就是端口最后设置的生效。

一个端口可以属一个或多个 VLAN 的 tagged 成员，如果一个端口属于两个或多个 VLAN 的 tagged 成员时，这个端口又称为 VLAN 中继端口。一个端口可以同时属于一个 VLAN 的 untagged 成员和属于另外的一个或多个 VLAN 的 tagged 成员。

VLAN 中继

如果一个端口属于两个或多个 VLAN 的 tagged 成员，那么这个端口又称为 VLAN 中继端口。两个交换机之间可以以 VLAN 中继端口相连，这样两个交换机之间可以划分两个或多个共同的 VLAN。

如图 2 是一个 VLAN 中继的例子，两个交换机之间以 VLAN 中继端口相连，是 VLAN 2 和 VLAN 3 的中继端口，每个交换机划分为两个 VLAN，分别是 VLAN 2 和 VLAN 3，每个 VLAN 内有一个用户。这样，用户 1 可以与用户 3 通信，用户 2 可以与用户 4 通信，用户 1 和用户 3 不能与用户 2 和用户 4 通信。

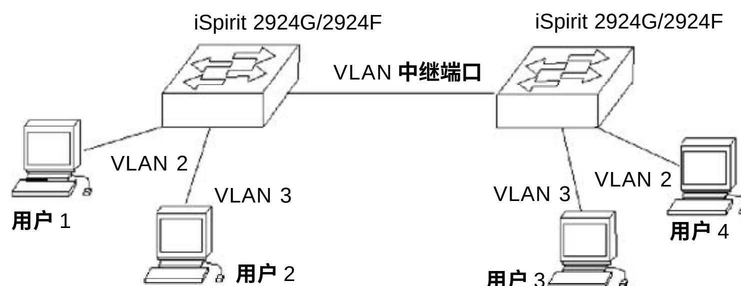


图 4-2 VLAN 中继端口

数据流在 VLAN 内的转发

当交换机从一个端口收到一个数据包时，根据以下步骤进行二层转发：

1.决定该数据包所属的VLAN。

2.判断该数据包是广播数据包、组播数据包还是单播数据包。

3.根据不同的数据包确定输出端口（可以是零个、一个或多个输出端口），如果没有输出端口，丢弃数据包。

4.根据输出端口在VLAN 内的成员类型决定发出去的包是否带标记。

5.从输出端口发送出去。

如何决定数据包的所属 VLAN 和协议 VLAN、PVID 的概念：

如果收到的数据包带标记并且标记中的 VID 字段非 0 时，该数据包所属的 VLAN 就是标记中 VID 值。

如果收到的数据包不带标记或带标记但标记中的VID 值为 0 时，如果输入端口是某个VLAN 的untagged 成员，而用户又想要确定此数据包的 VLAN 属性，此时就要依靠此端口的协议 VLAN 及 PVID 属性。

协议 VLAN。对于端口接收的 untagged 数据包，依照此数据包的协议类型判断它所从属的VLAN。

PVID。对于端口接收的 untagged 数据包，如果不能依照数据包的协议类型判断它所从属的VLAN 的属性配置，就用 PVID 决定它所从属的 VLAN。

对于端口的 untagged 数据包，决定了它所从属的 VLAN 后，就在此 VLAN 成员中进行转发或广播。

如何确定数据包的类型：

如果收到的数据包的目的MAC 地址是 FF:FF:FF:FF:FF:FF，则该数据包是广播数据包。

如果收到的数据包不是广播数据包且其目的 MAC 地址的第 40 位为 1，则该数据包是组播数据包。

如果既不是广播数据包又不是组播数据包，则该数据包为单播数据包。

如何决定数据包的输出端口：

如果输入的数据包是广播数据包，该数据包所属的 VLAN 的所有成员端口就是数据包的输出端口。

如果输入的数据包是组播数据包，首先根据目的组播 MAC 地址和所属的 VLAN 查找二层硬件组播转发表，如果找到匹配的组播条目，则组播条目中的输出端口和所属 VLAN 中的成员端口中的共同端口（与操作）为数据包的输出端口，如果没有共同的端口，该数据包丢弃。如果在二层硬件组播转发表中没有找到匹配的组播条目，根据二层硬件组播转发表的转发模式决定输出端口，如果是未注册组播转发模式，组播包当作广播处理，所属的VLAN 的所有成员端口就是数据包的输出端口，如果是注册转发模式，则没有输出端口，数据包丢弃。

如果输入的数据包是单播数据包，首先根据目的 MAC 地址和所属的 VLAN 查找二层硬件转发表，如果找到匹配的条目，则条目中的输出端口与所属 VLAN 的成员端口中的共同端口（与操作）为数据包的输出端口，如果没有共同的端口，该数据包丢弃。如果在二层硬件转发表中没有找到匹配的条目，该数据包当作广播包处理，所属的 VLAN 的所有成员端口就是数据包的输出端口。

发送数据包：

决定了输入的数据包的输出端口后要把数据包从所有的输出端口发送出去。

如果某个输出端口是数据包所属的 VLAN 的 untagged 成员，则数据包从该输出端口发送出去时不带标记。

如果某个输出端口是数据包所属的 VLAN 的 tagged 成员，则数据包从该输出端口发送出去时带标记，标记中的 VID 值是数据包所属的 VLAN 的值。

VLAN 与私有 VLAN 的关系

因为 iSpirit2924G/2924F 上实现了私有 VLAN，所以 VLAN 有称为普通 VLAN。普通 VLAN 和私有 VLAN 之间存在着一定的互斥的关系。

普通 VLAN 中的一个 VLAN 就是一个广播域，每个 VLAN 可以创建一个子网，VLAN 间通信必须通过三层转发。而私有 VLAN 中一个私有 VLAN 组才是一个广播域，每个私有 VLAN 组可以创建一个子网，在私有 VLAN 组的主 VLAN 之上创建子网，私有 VLAN 组间通信必须通过三层转发，而私有 VLAN 组内通信则是二层转发。

在创建普通 VLAN 时，要保证该 VLAN 不在任何私有 VLAN 组中的 VLAN 范围内，如果该 VLAN 在私有 VLAN 组的 VLAN 范围内，则创建不成功。

如果私有 VLAN 组中要设置的混杂端口、共用端口或隔离端口是某个普通 VLAN 的 untagged 成员，则要从该普通 VLAN 中清除该端口，即该端口不再属于该普通 VLAN 的 untagged 成员。

在设置普通 VLAN 的端口成员时，如果一个端口被私有 VLAN 组占用，则该端口不能设置成该 VLAN 的 untagged 成员，但是该端口可以设置成该 VLAN 的 tagged 成员。

在使用命令 show vlan 显示 VLAN 的信息时，只能显示普通 VLAN 的信息，不能显示私有 VLAN 的信息，需要使用 show privatevlan 显示私有 VLAN 的信息。配置私有 VLAN 之前，要去掉私有 VLAN 的相关端口的协议 VLAN 配置。

VLAN 的数量

在 iSpirit2924G/2924F 交换机上一个 VLAN 是一个广播域， iSpirit 2924G/2924F 交换机上最多可划分 255 个 VLAN。

4.2 VLAN 配置

为了使用户能够更加方便地配置 VLAN 功能，iSpirit2924G/2924F 交换机提供了多样化的命令，这些命令主要在 VLAN 配置模式和 PORT RANGE 配置模式之下。

iSpirit2924G/2924F 交换机缺省情况下有一个 VLAN 1，所有的端口是 VLAN 1 的 untagged 成员。

本节对 VLAN 的配置进行详细的介绍，主要包括以下内容：

- 创建和删除 VLAN
- 配置 VLAN 的 untagged 成员
- 配置 VLAN 的 tagged 成员
- 显示 VLAN 的信息

创建和删除 VLAN

iSpirit2924G/2924F 交换机可以一次创建一个或多个连续的 VLAN。下面的命令在全局 CONFIG 模式下创建 VLAN。如果输入 vlanid，此时只创建一个 VLAN，并进入 VLAN 配置模式，如果该 VLAN 已经存在了，则不创建，只进入 VLAN 配置模式。

vlan <vlanid>

iSpirit2924G/2924F 交换机可以一次删除一个 VLAN。如果一个 VLAN 被删除，该 VLAN 内的成员关系全部消失：

no vlan <vlanid>

注意：

如果一个 VLAN 已经被私有 VLAN 占用，则该 VLAN 不能被创建和删除。

配置 VLAN 的 untagged 成员

iSpirit2924G/2924F 交换机支持在 VLAN 配置模式下设置 VLAN 的 untagged 成员端口。

下面的命令在 VLAN 配置模式下增加 VLAN 的 untagged 成员端口：

untagged <A，A-B PORT NUMBER>

下面的命令在 VLAN 配置模式下删除 VLAN 的 untagged 成员端口：

no untagged <A，A-B PORT NUMBER>

注意：

1、如果一个端口已经被私有 VLAN 占用，则该端口不能成为 VLAN 的 untagged 成员。

2、如果一个端口已经属于一个 VLAN 的 untagged 成员，则要从该 VLAN 中清除该端口，该端口不再属于该 VLAN 的成员。

配置 VLAN 的 tagged 成员

iSpirit2924G/2924F 交换机支持在 VLAN 配置模式下设置一个或多个 VLAN 的 tagged 成员端口。

下面的命令在 VLAN 配置模式下增加 VLAN 的 tagged 成员端口：

tagged <p1-p2>

下面的命令在 VLAN 配置模式下删除 VLAN 的 tagged 成员端口：

no tagged <p1-p2>

显示 VLAN 的信息

iSpirit2924G/2924F 交换机支持在多个模式下显示 VLAN 的信息，包括 VLAN 的总体信息和 VLAN 内的端口成员信息。

下面的命令显示 VLAN 的信息，如果没有输入任何参数，则列出所有的 VLAN 的总体信息，如果有输入参数，则显示一个或多个 VLAN 的端口成员信息：

show vlan <vlanid>

协议 VLAN 的配置

配置私有 VLAN 之前，要去掉私有 VLAN 的相关端口的协议 VLAN 配置。

协议 VLAN 的配置流程为：1、配置协议分类定义。2、把协议分类和端口的 VLAN 属性进行绑定。

一、协议分类的定义。

1、在全局模式下进入协议分类的定义模式。

RPOTOCOL DEFINITION <PROTOCOL CLASSID>

PROTOCOL CLASSID：此协议分类的 ID 编号。

2、定义协议的类型。

TYPE <TYPE> [SUB TYPE]

TYPE 说明：IPX、APPLETALK、ethernetII、rfc1042snap、8021hsnap、llc

SUBTYPE 说明：对于 ethernetII、rfc1042snap、8021hsnap、llc 类型，给出报文的协议字段的 16 位值。

3、定义此协议分类的名称（可选）。

NAME <name>

4、使能此协议分类。

ENABLE

5、显示协议分类定义。

SHOW PROTOCOL DEFINITION

二、协议分类和端口的 VLAN 属性进行绑定。

1、如下命令进行协议分类和端口的 VLAN 属性进行绑定

PROTOCOL VLAN <VLANID> <A-B A PORT LIST> <PROTOCOL CLASSID> [VLAN PRIORITY]

2、如下命令解除协议分类和端口的 VLAN 属性进行绑定

NO PROTOCOL VLAN <PORT NUMBER> <PROTOCOL CLASSID>

3、如下命令显示协议分类和端口的 VLAN 属性进行绑定

SHOW PROTOCOL VLAN

PVID 的配置

1、PVID 的配置首先要进入端口配置模式：

PORT <A，A-B PORT LIST>

A 为要配置的单个端口的编号，A、B 为要配置的多个端口的编号范围。

2、配置 A 或 A-B 编号范围内的端口的 PVID。

PVID <VLAN ID>

3、显示 PVID 配置

SHOW PORT <[A，A-B PORT LIST>

端口的 Ingress filtering 的 VLAN 属性的配置

当数据包的 VLAN 属性不属于此端口时，iSpirit2924G/2924F 交换机的每个端口可以过滤丢弃此数据包。

1、Ingress filtering 的配置首先要进入端口配置模式：

PORT <A，A-B PORT LIST>

A 为要配置的单个端口的编号，A、B 为要配置的多个端口的编号范围。

2、配置 A 或 A-B 编号范围内的端口的 Ingress filtering。

ingress-filtering

3、显示 PVID 配置

SHOW PORT <A，A-B PORT LIST>

端口的 acceptable frame-type 的 VLAN 属性的配置

通过配置，iSpirit2924G/2924F 交换机可以接收所有的数据包或者仅仅 tagged 报文。

1、acceptable frame-type 的配置首先要进入端口配置模式：

PORT <A，A-B PORT LIST>

A 为要配置的单个端口的编号，A、B 为要配置的多个端口的编号范围。

2、配置 A 或 A-B 编号范围内的端口的 acceptable frame-type。

acceptable frame-type <TYPE>

TYPE 说明：ALL

TAGGED

3、显示 acceptable frame-type 配置

SHOW PORT <A，A-B PORT LIST>

保护 VLAN 的配置

iSpirit2924G/2924F 交换机可以配置一个 VLAN，这个 VLAN 的除指定的上联端口所有成员端口之间是相互隔离的，他们仅仅能和上联端口通信。

1、创建保护 VLAN 的配置：

protect vlan <vlanid><A uplink port number>

vlanid：选定的保护 VLAN 的编号。

A ：上联端口号。

2、清除保护 VLAN 的配置

no protect vlan <vlanid>

vlanid：选定的保护 VLAN 的编号。

3、显示保护 VLAN 的配置

show protect vlan

保护 VLAN 的配置实例

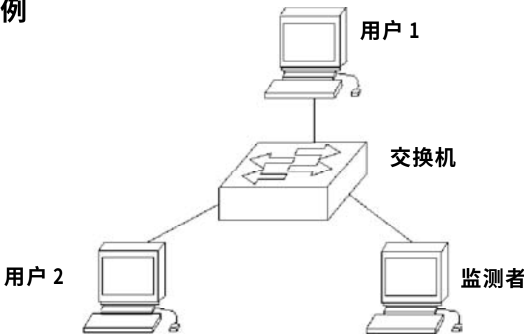


图 4-3 保护 VLAN 的配置实例

三个用户都在同一个 Vlan1 内，三个用户的连接方式和配置如表所示：

用户名称	所属Vlan	连接端口
用户1	1	1
用户2	1	2
用户3	1	3

为了使用户 1 **和用户** 2 **不能够相互通信，但是都能够和拥护** 3 **进行通信，所以要使用到保护** Vlan **的功能。**
设置 vlan 1 **为保护** VLan **，并且上联端口是** 3
Switch# protect vlan 1 3

查看交换机的保护 Vlan **的设置**
Switch# show protect vlan

protect vlan ID: 1
protect vlan status: active
protect vlan uplink port: 3

4.3 VLAN 配置实例

1 、**基于** PORT **的** VLAN

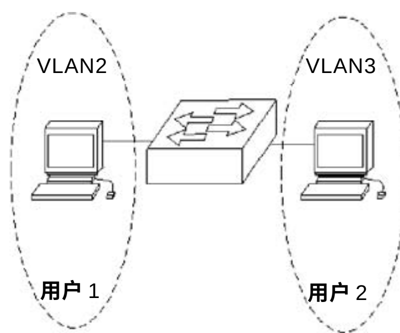


图 4-4 **基于** PORT **的** VLAN **配置实例**

有两个用户，用户 1 **和用户** 2**，两个用户由于所使用的网络功能和环境不同，需要分别处于不同的** VLAN **中。用户** 1 **在** VLAN2**，连接** 2924G/2924F **的端口** 2**，用户** 2 **在** VLAN3**，连接端口** 3**。需要在** 2924G/2924F **上设置：**

```
Switch# vlan 2
Vlan 2 added
Switch(vlan-2)#exit
Switch# vlan 3
Vlan 3 added
Switch(vlan-3)# vlan 2
Switch(vlan-2)# untag 2
Switch(vlan-2)# vlan 3
Switch(vlan-3)# untag 3
Switch(vlan-3)# exit
```

排 错 ：

如果配置后，发现不同 VLAN **之间的** PC **机不能通信，那是正常现象，因为不同** VLAN **之间要进行通信，必须要经过三层的路由转发。**

如果同一 VLAN **内的** PC **机不能进行通信，须作以下验证：**

1**、查看有整体有哪些** VLAN
Switch# show vlan

```
————————————————————————————
|VID |Name                          | Status |
|——+——————————————————+————|
|1   |Default VLAN 1                | Static |
|————————————————————————————|
|2   |vlan2                         | Static |
|————————————————————————————|
|3   |vlan3                         | Static |
|————————————————————————————|
```

2、查看连接特定 PC 机的端口是否在那个 VLAN 内，并且是以"U"的形势加入的

```
Switch# show vlan 2
Vlan ID:        2
Vlan Name:      vlan2
Vlan Status:    Static
                    (-=None, M=Member, F=Forbidden, U=Untagged)
——————————————————————————————————————-
|  Port Number   |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|2|2|
|                 |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|
|———————+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|  Configuration  |-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
——————————————————————————————————————-

Switch# show vlan 3

Vlan ID:        3
Vlan Name:      vlan3
Vlan Status:    Static
                    (-=None, M=Member, F=Forbidden, U=Untagged)
——————————————————————————————————————-
|  Port Number   |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|2|2|
|                 |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|
|———————+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|  Configuration  |-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
——————————————————————————————————————-
```

3、 查看那个特定的端口，端口的 pvid 号必须和端口所在 vlan 的号码一致
如例，端口 2 在 vlan 2 中，端口 2 的 pvid 号为 2 。

```
Switch# show port 2
 Unit                  :  1
 Port                  :  2
 ifIndex               :  0x2100002
 State                 :  Enable
 Set Speed             :  autonegotiate
 Actual Speed          :  unknown
 STP State             :  Disabled
 Link                  :  Down
 MacLearn              :  Unlock
 PortVlanID            :  2
```

```
 PortDefaultPriority          :  0
 DropEvents                   :  0

Switch# show port 3
 Unit                         :  1
 Port                         :  3
 ifIndex                      :  0x2100003
 State                        :  Enable
 Set Speed                    :  autonegotiate
 Actual Speed                 :  unknown
 STP State                    :  Disabled
 Link                         :  Down
 MacLearn                     :  Unlock
 PortVlanID                   :  3
 PortDefaultPriority          :  0
 DropEvents                   :  0
```

4、基于 802.1Q 的 vlan

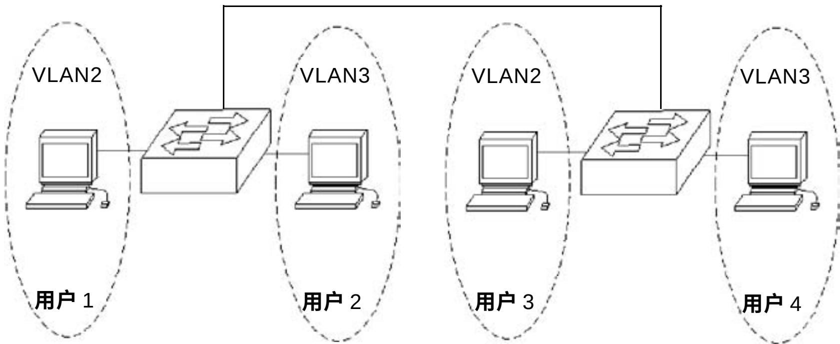


图 4-5　基于 802.1Q 的 VLAN 配置实例

有两台 2924G/2924F 交换机分别连接两个用户。表 4-1 列出了两台交换机分别连接两个用户的配置需求

表 4-1：

<table>
<tr><th>客户名称</th><th>连接的交换机</th><th>连接交换机端口</th><th>所属vlan</th><th>级联端口</th></tr>
<tr><td>用户1</td><td>交换机1</td><td>2</td><td>Vlan 2</td><td rowspan="2">25</td></tr>
<tr><td>用户2</td><td>交换机1</td><td>3</td><td>Vlan 3</td></tr>
<tr><td>用户3</td><td>交换机2</td><td>2</td><td>Vlan 2</td><td rowspan="2">25</td></tr>
<tr><td>用户4</td><td>交换机2</td><td>3</td><td>Vlan 3</td></tr>
</table>

需要在两台交换机上做配置：

交换机 1 ：

```
witch# vlan 2
Vlan 2 added
Switch(vlan-2)# untag 2
Switch(vlan-2)# tag 25
Switch(vlan-2)# exit
Switch# vlan 3
Vlan 3 added
Switch(vlan-3)# untag 3
Switch(vlan-3)# tag 25
Switch(vlan-3)# exit
```

交换机 2 ：

witch# vlan 2
Vlan 2 added
Switch(vlan-2)# untag 2
Switch(vlan-2)# tag 25
Switch(vlan-2)# exit
Switch# vlan 3
Vlan 3 added
Switch(vlan-3)# untag 3
Switch(vlan-3)# tag 25
Switch(vlan-3)# exit

排 错 ：

跨交换机的 vlan**，在同一个** vlan **内的** pc **机都能够通信的，如果不能相同，**
须查看如下：

1、**连接** pc **机的端口是以** "u" **模式加入这个** vlan **的，并且端口的** pvid **号和** vlan **号应该一致**
2、**级联端口是加入到每一个** vlan **中的，并且在每一个** vlan **内都是以** "M" **模式加入的，并且端口的** pvid **号为** 1。

Switch# show vlan

```
————————————-————————————-
|VID |Name                    | Status |
|——+————————————————+————|
|1   |Default VLAN 1          | Static |
|——————————————————————————|
|2   |vlan2                   | Static |
|——————————————————————————|
|3   |vlan3                   | Static |
|——————————————————————————|
```

注意每个交换机的端口 2 **的** pvid **号为** 2**，端口** 3 **的** pvid **号为** 3**，**
级联端口 25 **的** pvid **还是为** 1

3、**基于协议的** VLan

在一个交换机内，需要根据不同的三层协议来进行 Vlan **的划分，比如，运行** Appletalk **协议的** PC **机属于同一个** Vlan **内，而运行** IPX **协议的** PC **机属于另一个** VLan **内。**

首先，设置要进行 VLan **划分的三层协议**

Switch# protocol definition 1
Switch(protocol-1)# type ipx
Switch(protocol-1)# enable **（启用协议）**

然后进行查看

Switch# show protocol definition

protocol ID: 1
protocol status: active
protocol type: ipx
protocol subtype: 0x0000
protocol name: ipx

创建 Appletalk **协议**

Switch# protocol definition 2
Switch(protocol-2)# type appletalk
Switch(protocol-2)# enable **（启用** appletalk **议）**

然后进行查看

```
Switch# show protocol definition 2

protocol ID:            2
protocol status:        active
protocol type:          appletalk
protocol subtype:       0x0000
protocol name:          appletalk
```

创建用于 IPX **协议的** Vlan 2 **和用于** Appletalk **协议的** Vlan 3

```
Switch# vlan 2
Switch(vlan-2)# untag 1-24
Switch(vlan-2)# vlan 3
 Vlan 3 added
Switch(vlan-3)# untag 1-24
Switch(vlan-3)# exit
```

然后把 Vlan 2 **和** IPX **协议进行绑定，把** VLan 3 **和** Appletalk **协议进行绑定**

```
Switch# protocol vlan 2 1-24 1  IPX
Switch# protocol vlan 3 1-24 2  Appletalk
```

查看协议 VLan

Switch# show protocol vlan 1 (**端口** 1 **的所属协议** Vlan)

```
protocol vlan protocol ID:      1
protocol vlan status:           active
protocol vlan VLAN ID:          2
protocol vlan priority:         0

protocol vlan protocol ID:      2
protocol vlan status:           active
protocol vlan VLAN ID:          3
protocol vlan priority:         0
```

第 5 章 私有 VLAN 配置

本章对私有 VLAN 技术及配置进行详细的描述，主要包括以下内容：

1、**私有** VLAN **介绍**

2、**私有** VLAN **配置**

3、**私有** VLAN **配置示例**

在实际的应用中，为了保证公用数据的共享和私有数据的安全，二层的端口隔离技术使用得非常多。为了能够让用户使用端口隔离技术并且能够更加简便地配置端口隔离，联想网络推出了私有 VLAN 的概念并在 iSpirit2924G/2924F 交换机上实现。

私有 VLAN 由多个连续的 VLAN（VLAN ID 是连续的）组成，通过端口的划分，在一个广播域中实现二层的端口隔离。使用私有 VLAN 技术，只需要掌握私有 VLAN 的几个概念，配置端口隔离就非常简单。

注意：配置私有 VLAN 时，要先去掉私有 VLAN 相关端口的协议 VLAN 的配置。

本章对私有 VLAN 技术及配置进行详细的描述，主要包括以下内容：

- 私有 VLAN 介绍
- 私有 VLAN 配置
- 私有 VLAN 配置示例

5.1 私有 VLAN 介绍

iSpirit2924G/2924F 交换机实现了 12 组私有 VLAN，每一组私有 VLAN 是一个广播域，也就是说一组私有 VLAN 只能创建一个子网，内部由多个连续的 VLAN 组成，实现内部的端口隔离。私有 VLAN 组间是不同的广播域，也就是说是不同的子网网段，私有 VLAN 组间必须通过三层转发通信。

本节对私有 VLAN 进行一个详细的描述，主要包括以下内容：

1.私有 VLAN 的端口类型

2.私有 VLAN 的 VLAN 范围

3.私有 VLAN 和普通 VLAN 的关系

4.私有 VLAN 的子网

1.私有 VLAN 的端口类型

私有 VLAN 有三种类型的端口：混杂端口、共用端口和隔离端口。混杂端口是私有 VLAN 组中的上连端口，而共用端口和隔离端口是被隔离的对象。

混杂端口是私有 VLAN 组中的上连端口，一个私有 VLAN 组中有一个或多个混杂端口，而且一个私有 VLAN 组中必须要有至少一个混杂端口。混杂端口可以与该私有 VLAN 组的任何端口（包括混杂端口、共用端口和隔离端口）进行二层通信。在实际应用中，一般公用的数据服务器和互联网的出口与混杂端口相连。

共用端口是私有 VLAN 组中被隔离的对象。共用端口有组的概念，一个或多个共用端口组成一个共用端口组，iSpirit2924G/2924F 交换机中的一个私有 VLAN 组最多支持 6 个共用端口组。共用端口能够与混杂端口和共用端口组内的其它共用端口通信，共用端口不能与隔离端口和其它共用端口组中的端口通信。如果一个共用端口组中只有一个端口，该共用端口组实质就是一个隔离端口。

隔离端口是私有 VLAN 组中被隔离的对象，隔离端口没有组的概念，隔离端口之间都是互相隔离的。隔离端口只能与混杂端口通信，不能与其它隔离端口和共用端口通信。

一个私有 VLAN 中必须要有被隔离的对象，一个私有 VLAN 组中必须至少要有一个隔离端口或一个共用端口组。一个私有 VLAN 组中可以没有隔离端口，但此时一定有一个或多个共用端口组。一个私有 VLAN 组中可以没有共用端口组，但此时一定有一个或多个隔离端口。如果一个私有 VLAN 组中只有一个隔离端口或一个共用端口组，实际上也起不到隔离的效果，因此在实际应用中，一个私有 VLAN 组中至少有两个被隔离的对象。

私有 VLAN 组内的端口不能重叠，也就是说一个端口只能是隔离端口、共用端口和混杂端口中的一种，如果一个端口是共用端口，不能与共用端口组内的其它端口或其它共用端口组的端口相同。私有 VLAN 组间的端口不能重叠，也就是说一个端口只能属于一个私有 VLAN 组。

如图 5-1 所示是一个私有 VLAN 组的例子，端口 1-6 和 10-12 属于一个私有 VLAN 组，端口 1 和端口 2 是隔离端口，端口 3、4、5 和 6 是共用端口，其中端口 3 和 4 是一个共用端口组，端口 5 和 6 是一个共用端口组，端口 10、11 和 12 是混杂端口。用户 1 和用户 2 只能访问服务器 1、服务器 2 和互联网，用户 1 和用户 2 之间不能通信，用户 1 和用户 2 不能与用户 3 到 6 通信。用户 3 和用户 4 可以访问服务器 1、服务器 2 和互联网，用户 3 和用户 4 之间可以通信，用户 3 和用户 4 不能与用户 1 到 2、用户 5 到 6 通信。用户 5 和用户 6 可以访问服务器 1、服务器 2 和互联网，用户 5 和用户 6 之间可以通信，用户 5 和用户 6 不能与用户 1 到 4 通信。服务器 1 和服务器 2 可以和用户 1 到 6 通信，可以访问互联网，服务器 1 和服务器 2 之间可以通信。

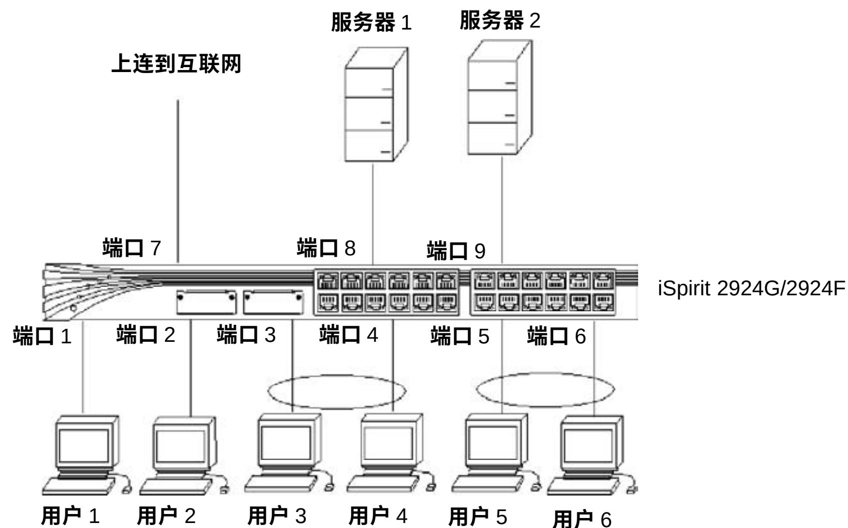


图 5-1 一个私有 VLAN 组

如图 5-2 所示是两个私有 VLAN 组的例子，私有 VLAN 组 1 包括端口 1-3 和端口 11，私有 VLAN 组 2 包括端口 5-7 和端口 12。在私有 VLAN 组 1 中，端口 1 是隔离端口，端口 2 和 3 是共用端口，端口 2 和 3 组成一个共用端口组，端口 11 是混杂端口。在私有 VLAN 组 2 中，端口 5 是隔离端口，端口 6 和 7 是共用端口，端口 6 和 7 组成一个共用端口组，端口 12 是混杂端口。在私有 VLAN 组 1 中，用户 1 只能与服务器 1 通信，用户 1 不能与用户 2 到 3 通信，用户 2 和用户 3 可以与服务器 1 通信，并且用户 2 和用户 3 能够互相通信，但不能与用户 1 通信。在私有 VLAN 组 2 中，用户 4 只能与服务器 2 通信，用户 4 不能与用户 5 到 6 通信，用户 5 和用户 6 可以与服务器 2 通信，并且用户 5 和用户 6 能够互相通信，但不能与用户 4 通信。私有 VLAN 组 1 中的设备要和私有 VLAN 组 2 中的设备通信必须要通过三层转发。

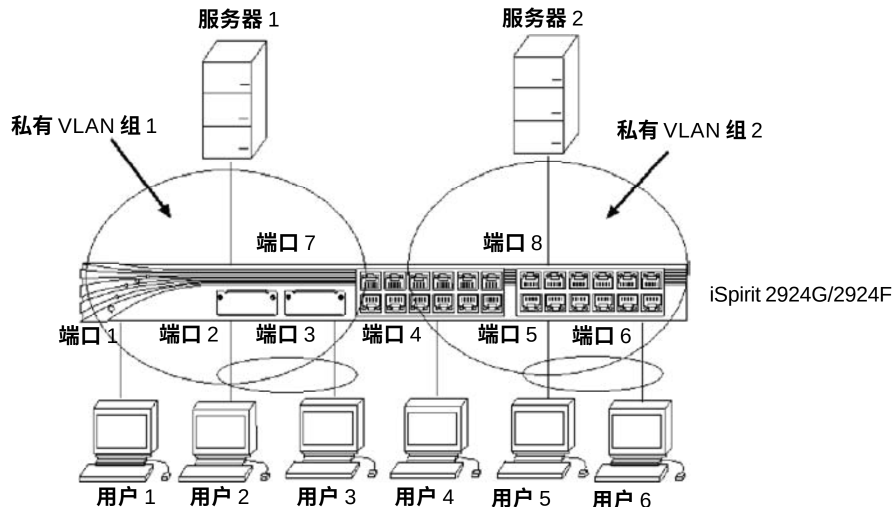


图 5-2 两个私有 VLAN 组

注意：由于端口的协议 VLAN 会破坏私有 VLAN 的功能，在配置私有 VLAN 前，去掉私有 VLAN 内的所有端口的协议 VLAN 属性。

2.私有 VLAN 的 VLAN 范围

一个私有 VLAN 组是由连续的多个 VLAN 组成。在建立一个私有 VLAN 组时，需要选择 VLAN ID 是连续的多个 VLAN，私有 VLAN 组中的多个 VLAN 共享一个广播域，属于同一个子网，私有 VLAN 组间的通信必须通过三层转发。私有 VLAN 组间的 VLAN 不能重叠， 例如一个私有 VLAN 组选择 VLAN 10 到 19 作为该组内的 VLAN，那另一个私有 VLAN 组的 VLAN 范围不能包括 VLAN 10 到 19 的任何一个。

每一个私有 VLAN 组都有唯一的一个主 VLAN，主 VLAN 必须在私有 VLAN 组内的 VLAN 范围内，可以从此 VLAN 范围内任意选择一个 VLAN 作为主 VLAN。例如一个私有 VLAN 组选择 VLAN 10 到 19 作为该组内的 VLAN，那么可以选择 VLAN 10 到 19 中的任意一个作为主 VLAN。主 VLAN 的用处是为了创建私有 VLAN 组的子网，因为一个私有 VLAN 组只能有一个子网，所以直接在主 VLAN 上创建私有 VLAN 组的子网，私有 VLAN 组内的其它 VLAN 不能创建子网。

在选择私有 VLAN 组内的 VLAN 范围时，VLAN 范围要足够大，否则私有 VLAN 组最后不能生效。私有 VLAN 组内的 VLAN 范围是由隔离端口和共用端口组的个数决定的，一个隔离端口要占用一个 VLAN，一个共用端口组要占用一个 VLAN。可以得到私有 VLAN 组内的 VLAN 范围的一个等式：

（私有 VLAN 组内的 VLAN 个数 >= 私有 VLAN 组内的隔离端口个数
+ 私有 VLAN 组内的共用端口组个数 + 1）

例如图 1，私有 VLAN 组内的隔离端口个数是 2 个，共用端口组个数是 2 个，所以私有 VLAN 组内的 VLAN 个数最少要 5 （2+2+1）个。

私有 VLAN 组内的 VLAN 个数有一个最大上限值，不能超过 26 个，因为 iSpirit2924G/2924F 交换机的端口个数为 26 个，可以满足应用上的任何要求。

3.私有 VLAN 和普通 VLAN 的关系

普通 VLAN 中的一个 VLAN 就是一个广播域，每个 VLAN 可以创建一个子网，VLAN 间通信必须通过三层转发。而私有 VLAN 中一个私有 VLAN 组才是一个广播域，每个私有 VLAN 组可以创建一个子网，在私有 VLAN 组的主 VLAN 之上创建子网，私有 VLAN 组间通信必须通过三层转发，而私有 VLAN 组内通信则是二层转发。

在选择私有 VLAN 组的 VLAN 范围时，要保证该 VLAN 范围中的任何一个 VLAN 都没有被普通 VLAN 占用，如果被占用，则 VLAN 范围选择不成功。在创建普通 VLAN 时，要保证该 VLAN 不在任何私有 VLAN 组中的 VLAN 范围内，如果该 VLAN 在私有 VLAN 组的 VLAN 范围内，则创建不成功。

如果私有 VLAN 组中要设置的混杂端口、共用端口或隔离端口是某个普通 VLAN 的 untagged 成员，则要从该普通 VLAN 中清除该端口，即该端口不再属于该普通 VLAN 的 untagged 成员。

在设置普通 VLAN 的端口成员时，如果一个端口被私有 VLAN 组占用，则该端口不能设置成该 VLAN 的 untagged 成员，但是该端口可以设置成该 VLAN 的 tagged 成员。

在使用命令 show vlan 显示 VLAN 的信息时，只能显示普通 VLAN 的信息，不能显示私有 VLAN 的信息，需要使用 show privatevlan 显示私有 VLAN 的信息。

4.私有 VLAN 的子网

一个私有 VLAN 组是一个广播域，只能创建一个子网，而且必须在主 VLAN 上创建子网，私有 VLAN 组内的其它 VLAN 不能创建子网。如果一个交换机上有一个私有 VLAN 组，并且创建了子网，只有与混杂端口相连的设备在该子网内能够与该交换机通信，而与隔离端口和共用端口相连的设备在该子网内不能与该交换机通信。在实际应用中，不能把网管工作站建立在私有 VLAN 组的隔离端口或共用端口之下，而必须把网管工作站建立在混杂端口之上。

5.2 私有 VLAN 配置

为了让用户配置私有 VLAN 更加方便，iSpirit2924G/2924F 交换机在 CLI 上提供了一个 PRIVATE VLAN 模式，进入 PRIVATE VLAN 模式对一组私有 VLAN 进行配置，私有 VLAN 配置的大部分命令都在 PRIVATE VLAN 模式下运行。

iSpirit 2924G/2924F 交换机缺省情况下所有的私有 VLAN 组都没有配置任何的 VLAN 和端口。

本节描述私有 VLAN 的配置，主要包括以下内容：

- 配置私有 VLAN 组

- 配置私有 VLAN 组内的 VLAN
- 配置私有 VLAN 组内的隔离端口
- 配置私有 VLAN 组内的共用端口
- 配置私有 VLAN 组内的混杂端口
- 使私有 VLAN 组生效和失效
- 显示私有 VLAN 组信息

配置私有 VLAN 组

要对私有 VLAN 进行配置，首先要选择一个私有 VLAN 组并进入 PRIVATE VLAN 模式。

下面的命令在全局 CONFIG 模式下选择一个私有 VLAN 组并进入 PRIVATE VLAN 模式，group-id 值为 1 到 12，表示私有 VLAN 组号：

privatevlan <group-id>

下面的命令在全局 CONFIG 模式下删除一个私有 VLAN 组，group-id 值为 1 到 12，表示私有 VLAN 组号：

no privatevlan <group-id>

配置私有 VLAN 组内的 VLAN

选择了一个私有 VLAN 组并进入 PRIVATE VLAN 模式后，需要选择私有 VLAN 组的 VLAN 范围和主 VLAN。在配置之前，要根据规划计算好需要的 VLAN 个数。

下面的命令在 PRIVATE VLAN 模式下选择私有 VLAN 组的 VLAN 范围和主 VLAN，VLAN 范围用最小 VLAN ID 号到最大 VLAN ID 号表示：

vlan <min-vlanid> <max-vlanid> <primary-vlanid>

注 意 ：

如果该命令配置不成功，有以下几种可能性：

1、min-vlanid 值比 max-vlanid 大。

2、primary-vlanid 不在 min-vlanid 到 max-vlanid 范围内。

3、max-vlanid 值减 min-vlanid 大于 26。

4、min-vlanid 值到 max-vlanid 的 VLAN 范围有至少一个 VLAN 被普通 VLAN 占用。

5、私有 VLAN 组与其它的私有 VLAN 组有 VLAN 范围重叠的现象。

6、该私有 VLAN 组处于生效（active）状态。

配置私有 VLAN 组内的隔离端口

下面的命令在 PRIVATE VLAN 模式下配置一个或多个隔离端口：

isolate {<p>|<p1-p2>} [<p>|<p1-p2>] …

下面的命令在 PRIVATE VLAN 模式下清除一个或多个隔离端口，如果被输入的端口不是隔离端口，则对该端口不做任何动作：

no isolate {<p>|<p1-p2>} [<p>|<p1-p2>] …

注 意 ：

1、如果私有 VLAN 组处于生效（active）状态，命令不能设置成功。

2、一个私有 VLAN 组可以不配置隔离端口，但此时需要有一个或多个共用端口组。

配置私有 VLAN 组内的共用端口

下面的命令在 PRIVATE VLAN 模式下配置一个共用端口组，一个共用端口组内可以选择一个或多个共用端口，community-id 是共用端口组号：

community <community-id> {<p>|<p1-p2>} [<p>|<p1-p2>] …

下面的命令在 PRIVATE VLAN 模式下删除一个共用端口组，此时该共用端口组内的所有共用端口都被清除：

no community <community-id>

注 意 ：

1、如果私有 VLAN 组处于生效（active）状态，命令不能设置成功。

2、一个私有 VLAN 组可以不配置共用端口组，但此时需要有一个或多个隔离端口。

配置私有 VLAN 组内的混杂端口

下面的命令在 PRIVATE VLAN 模式下配置一个或多个混杂端口：

promiscuous {<p>|<p1-p2>} [<p>|<p1-p2>] …

下面的命令在 PRIVATE VLAN 模式下清除一个或多个混杂端口，如果被输入的端口不是混杂端口，则对该端口不做任何动作：

no promiscuous {<p>|<p1-p2>} [<p>|<p1-p2>] …

注 意 ：

1、如果私有 VLAN 组处于生效（active）状态，命令不能设置成功。

2、一个私有 VLAN 组必须配置一个或多个混杂端口。

使私有 VLAN 组生效和失效

一个私有 VLAN 组配置了 VLAN 和端口后私有 VLAN 组并不立即生效，需要手工输入命令使该私有 VLAN 组生效 。

下面的命令在 PRIVATE VLAN 模式下使私有 VLAN 组生效：

enable

注 意 ：

如果私有 VLAN 组不能生效，有下面几种可能性：

1、私有 VLAN 组内的 min-vlanid、max-vlanid 或 primary-vlanid 有为 0 的情况。

2、私有 VLAN 组内的 VLAN 个数太少，VLAN 个数 < 隔离端口的个数 +
共用端口组的个数 + 1。

3、私有 VLAN 组内没有混杂端口。

4、私有 VLAN 组内既没有隔离端口又没有共用端口组。

5、私有 VLAN 组内混杂端口、共用端口和隔离端口有重叠的现象。

6、私有 VLAN 组与其它的私有 VLAN 组有混杂端口、共用端口和隔离端口重叠的现象。

如果私有 VLAN 组内的混杂端口、共用端口或隔离端口属于普通 VLAN 的 untagged 成员，则要从该普通 VLAN 中清除这些端口，是这些端口不属于该普通 VLAN 的成员。

下面的命令在 PRIVATE VLAN 模式下使私有 VLAN 组失效：

disable

注 意 ：

只有在私有 VLAN 组失效时，私有 VLAN 组内的配置才能修改，在私有 VLAN 组生效时，私有 VLAN 组内的配置不能修改，因此当私有 VLAN 组生效时想修改该私有 VLAN 组的配置，首先要使该私有 VLAN 组失效再进行配置，配置完后再使该私有 VLAN 组生效。

显示私有 VLAN 组信息

下面的命令在全局 CONFIG 模式或 PRIVATE VLAN 模式显示私有 VLAN 组的信息，group-id 值为 1 到 12，表示私有 VLAN 组号，如果不输入 group-id 参数，显示所有 12 组私有 VLAN 的配置信息，如果输入 group-id 参数，只显示指定的私有 VLAN 组的配置信息：

show privatevlan [group-id]

5.3 私有 VLAN 配置实例

如下图所示是一个私有 VLAN 组的例子，端口 1-9 属于一个私有 VLAN 组，端口 1 和端口 2 是隔离端口，端口 3、4、5 和 6 是共用端口，其中端口 3 和 4 是一个共用端口组，端口 5 和 6 是一个共用端口组，端口 7、8 和 9 是混杂端口。用户 1 和用户 2 只能访问服务器 1、服务器 2 和互联网，用户 1 和用户 2 之间不能通信，用户 1 和用户 2 不能与用户 3 到 6 通信。用户 3 和用户 4 可以访问服务器 1、服务器 2 和互联网，用户 3 和用户 4 之间可以通信，用户 3 和用户 4 不能与用户 1 到 2、用户 5 到 6 通信。用户 5 和用户 6 可以访问服务器 1、服务器 2 和互联网，用户 5 和用户 6 之间可以通信，用户 5 和用户 6 不能与用户 1 到 4 通信。服务器 1 和服务器 2 可以和用户 1 到 6 通信，可以访问互联网，服务器 1 和服务器 2 之间可以通信。

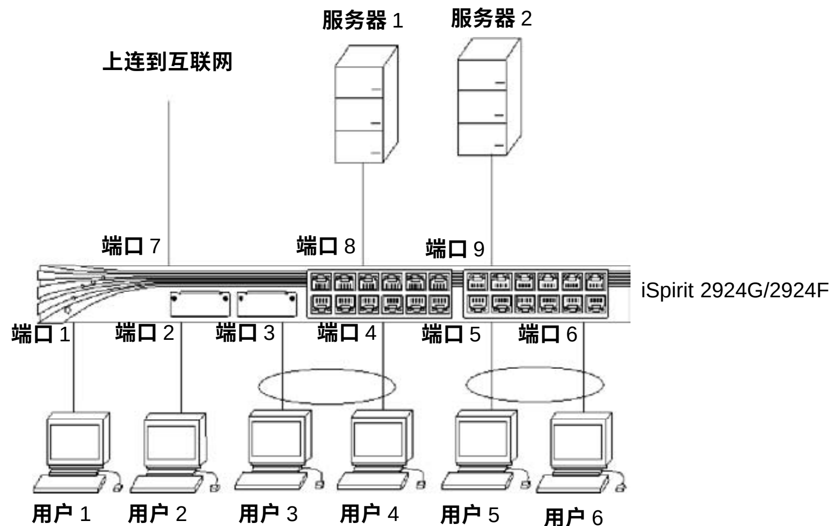


图 5-3 一个私有 VLAN 组

```
Switch# private 1                                进入私有 vlan 的配置模式
Switch(privatevlan-1)# vlan 2 6 2                配置私有 vlan 包含的 vlan 范围
Switch(privatevlan-1)# isolate 1-2               配置隔离端口
Switch(privatevlan-1)# community 1 3-4           配置公共端口
Switch(privatevlan-1)# community 2 5-6
Switch(privatevlan-1)# promiscuous 7-9           配置混杂端口
Switch(privatevlan-1)# enable                    启用私有 vlan

Switch# show privatevlan 1

    Private vlan group : 1
    status : active
    max vlan number : 6
    min vlan number : 2
    primary vlan number : 2
    promiscuit port : 7 8 9
    iSolatePort port : 1 2
    community 1 port : 3 4
    community 2 port : 5 6
```

排 错 ：

如果配置不成功可能有以下几个原因：

1、min-vlanid 值比 max-vlanid 大。

2、primary-vlanid 不在 min-vlanid 到 max-vlanid 范围内。

3、max-vlanid 值减 min-vlanid 大于 12。

4、min-vlanid 值到 max-vlanid 的 VLAN 范围有至少一个 VLAN 被普通 VLAN 占用。

5、私有 VLAN 组与其它的私有 VLAN 组有 VLAN 范围重叠的现象。

6、如果该私有 VLAN 组处于生效（active）状态，就不能够对该私有 vlan 做任何配置

7、私有 VLAN 所包含的 vlan 数至少应该大于等于私有 vlan 的（私有端口个数 + 公用端口组数 +1）

8、私有 VLAN 组内没有混杂端口。

9、私有 VLAN 组内既没有隔离端口又没有共用端口组。

10、私有 VLAN 组内混杂端口、共用端口和隔离端口有重叠的现象。

11、私有 VLAN 组与其它的私有 VLAN 组有混杂端口、共用端口和隔离端口重叠的现象。

12、如果私有 VLAN 组内的混杂端口、共用端口或隔离端口属于普通 VLAN 的 untagged 成员，则要从该普通 VLAN 中清除这些端口，是这些端口不属于该普通 VLAN 的成员

配置两个 VLAN 组

如下图所示是两个私有 VLAN 组的例子，私有 VLAN 组 1 包括端口 1-3 和端口 7，私有 VLAN 组 2 包括端口 4-6 和端口 8。在私有 VLAN 组 1 中，端口 1 是隔离端口，端口 2 和 3 是共用端口，端口 2 和 3 组成一个共用端口组，端口 7 是混杂端口。在私有 VLAN 组 2 中，端口 4 是隔离端口，端口 5 和 6 是共用端口，端口 5 和 6 组成一个共用端口组，端口 8 是混杂端口。在私有 VLAN 组 1 中，用户 1 只能与服务器 1 通信，用户 1 不能与用户 2 到 3 通信，用户 2 和用户 3 可以与服务器 1 通信，并且用户 2 和用户 3 能够互相通信，但不能与用户 1 通信。在私有 VLAN 组 2 中，用户 4 只能与服务器 2 通信，用户 4 不能与用户 5 到 6 通信，用户 5 和用户 6 可以与服务器 2 通信，并且用户 5 和用户 6 能够互相通信，但不能与用户 4 通信。私有 VLAN 组 1 中的设备要和私有 VLAN 组 2 中的设备通信必须要通过三层转发。

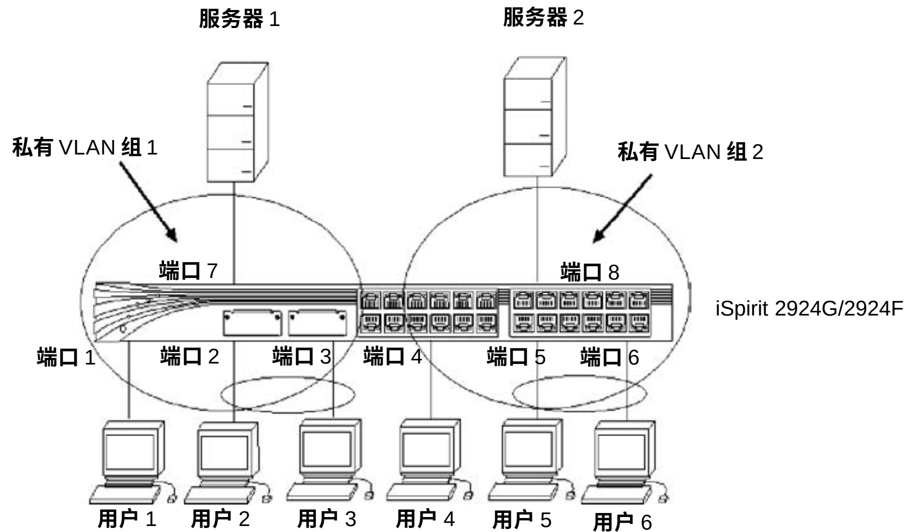


图 5-4 两个私有 VLAN 组

私有 VLAN 配置

配置私有 vlan 1

```
Switch# privatevlan 1
Switch(privatevlan-1)# vlan 1000 1002 1000
Switch(privatevlan-1)# isolate 1
Switch(privatevlan-1)# community 1  2-3
Switch(privatevlan-1)# promiscuous  7
Switch(privatevlan-1)# enable

Switch#  show privatevlan 1
    Private vlan group :  1
    status : active
    max vlan number : 1004
    min vlan number : 1000
    primary vlan number : 1000
```

```
    promiscuit port : 6
    iSolatePort port : 1
    community 1 port :  2  3
```

配置私有 vlan 2

```
Switch# privatevlan 2
Switch(privatevlan-1)# vlan 2000 2002 2000
Switch(privatevlan-1)# isolate  4
Switch(privatevlan-1)# community 1  5-6
Switch(privatevlan-1)# promiscuous  8
Switch(privatevlan-1)# enable

Switch#  show privatevlan 2
    Private vlan group :  2
    status : active
    max vlan number : 2002
    min vlan number : 2000
    primary vlan number : 2000
    promiscuit port : 8
    iSolatePort port : 4
    community 1 port :  5  6
```

第 6 章 配置 STP

本章对 STP **及其配置进行描述，主要包括以下内容：**

1、STP **介绍**

2、STP **配置**

3、STP **配置示例**

6.1 STP 介绍

联想天工 iSpirit 2924G/2924F 交换机支持 IEEE802.1d 标准的 STP 协议。STP 是运行在 Bridges 和 Switches 层上，符合 IEEE802.1d 协议标准兼容的第二层协议。这一协议提供了网络的动态冗余切换机制。因此使用 STP，可以让您在网络设计中部署备份线路，并且保证在主线路正常工作时，备份线路是关闭的。当主线路出现故障时，自动激活备份线路，将数据流切换到备份线路，保证设备正常运行。

由此可见，使用 STP，可以保证当在网络结构上存在冗余路径情况下，阻止网络回路发生。网络回路对网络来说是致命的打击，冗余链路作为网络备份路径又是非常重要的。通过交换机提供的命令可以实现该协议的功能。

6.2 STP 配置

交换机的 STP 功能配置分以下几个步骤：

- ●第一步：启用 S T P 协议；
- ●第二步：对 S T P 参数进行设置；

缺省情况下 STP 协议是关闭的，但交换机的所有端口的 STP 计算是打开的。只有在 STP 协议打开并且端口的 STP 计算也打开时，该端口才会真正加入到 STP 计算中，如果有一个条件没有满足，则端口不会加入 STP 计算。

➢ 在全局配置模式下打开或关闭 STP：

Switch# stp <enable> 或 no stp

如果键入 enable,表示 STP 有效，如果键入 no stp 则表示 STP 无效。

➢ 在全局配置模式下使能 STP 端口，使端口用于 STP 计算

enable stp ports <port|port1-port2> [port|port1-port2] …

➢ 在全局配置模式下关闭 STP 端口，使端口不用于 STP 运算

disable stp ports <port|port1-port2> [port|port1-port2] …

➢ 使能正在配置的 stp 端口，使端口用于 stp 计算

Switch(port(2-2))# stp port enable

➢ 关闭正在配置的 stp 端口，使端口不用于 stp 计算

Switch(port(2-2))# stp port disable

➢ 在全局配置模式下设置桥优先级，其默认值为 32768。

stp bridge priority <A>(说明：priority 的范围为 0~65535)

0 的优先级最高，65535 的优先级最低。

➢ 在 PORT RANGE 配置模式下设定端口优先级，其默认值为 128。

stp port priority <A> (说明：priority 的范围为 0~255)

➢ 在全局配置模式下设置桥的 BPDU 报文发送周期，默认值为 2 秒。

stp bridge hello-time <A>

➢ 在全局配置模式下设置 STP 的转发延迟时间，默认值 15 秒。

stp bridge forward-delay <A>

➢ 在全局配置模式下设置桥的 STP 配置信息的最大存活时间，默认值为 20 秒。

stp bridge max-age <A>

➢ 在全局配置模式下显示桥的 STP 信息

show stp bridge

➢ 在全局配置模式或 PORT RANGE 配置模式下显示某个端口的 STP 信息

show stp port<port>

6.3 STP 配置实例

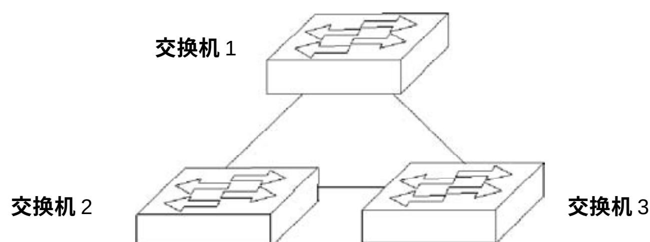


图 6-1 STP 配置实例

三台交换机连接成一个环状，需要打开每一台交换机的生成树协议，分别在每一台交换机上执行

Switch# stp enable <cr>

确认生成树协议在每一台交换机上是打开的

Switch# show sw

Ip Address	: 0.0.0.0
Subnet Mask	: 255.255.255.0
Default Gateway	: 0.0.0.0
MAC Address	: 00:de:ad:be:ef:00
BOOTP	: Disable
DHCP	: Disable
Spanning Tree	: Enable
Traffic Classes	: Disable
GVRP	: Disable
GMRP	: Disable
IGMP Snooping	: Disable
Reset	: no reset

这样生成树协议就能正常运行

如果需要关闭生成树协议的运行，需要输入命令

Switch# no stp

生成树协议的高级命令：

设置其中第一台交换机为根交换机，需要设置他的桥优先级比其他两个桥的优先级要小，默认优先级为 32768

Switch# stp bridge priority A stp bridge priority (0=<A<=65535)

使交换机的某个端口不参与生成树的运行，需要关闭端口的生成树功能

Switch# disable stp ports A-B or A port list (1=<A,B<=28)

排 错 ：

察看哪一个交换机被选为根网桥：

Switch# show stp bridge

— Designated Root Information —-

Priority	: 32768	
MAC Address	: 00:09:ca:01:75:02	**（根网桥配置状态）**
Hello Time	: 2s	
Forward Delay	: 15s	
Max Age	: 20s	

```
— Bridge STP Information —-
Bridge Priority           : 32768
MAC Address               : 00:09:ca:01:75:02        （本网桥配置状态）
Root Path Cost            : 0
Root Port                 : 0
Bridge Hello Time         : 2s
Bridge Forward Delay      : 15s
Bridge Max Age            : 20s
```

察看生成树中交换机的端口状态：

```
Switch# show stp port  A    port number (1=<A<=28)

Switch# show stp port 1
— Port Information —-
STP Port                  : Enable
Port ID                   : 1
Priority                  : 128
State                     : Disabled
Path Cost                 : 19
Designated Cost           : 0

— Designated Root Information —-
Priority                  : 32768
MAC Address               : 00:09:ca:01:75:02

— Designated Port Information —-
Port ID                   : 1
Priority                  : 128

— Designated Bridge Information —-
Priority                  : 32768
MAC Address               : 00:09:ca:01:75:02
```

第 7 章 配置二层静态组播

本章描述了二层静态组播的概念和配置，包括以下内容：

1、二层静态组播介绍

2、二层静态组播配置

3、二层静态组播配置示例

在城域网/Internet中，采用单播方式将相同的数据包发送给网络中的多个而不是全部接收者时，由于需要复制分组给每一个接收端点，随着接收者数量的增多，需要发出的包数也会线性增加，这使得主机、交换路由设备及网络带宽资源总体负担加重，效率受到极大影响。随着多点电视会议、视屏点播、群组通信应用等需求的增长，为提高资源利用率，组播方式日益成为多点通信中普遍采用的传输方式。

如图7-1是一个单播应用的例子，实现点到点的通信，如图2是一个组播应用的例子，实现点到多点的通信。图7-1和图7-2都是A发送相同内容的数据流给B和C，如果采用单播通信，A需要发送二个数据流，一个给B，一个给C，如果采用组播通信，A只需要发送一个数据流，B和C都会接收这个数据流。

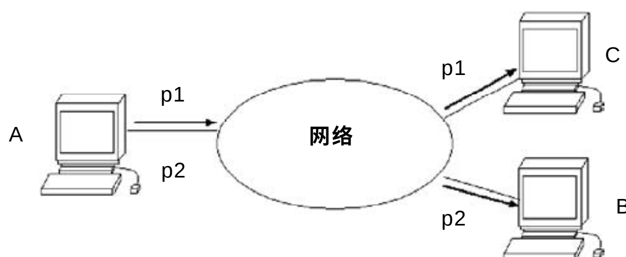


图7-1 单播应用

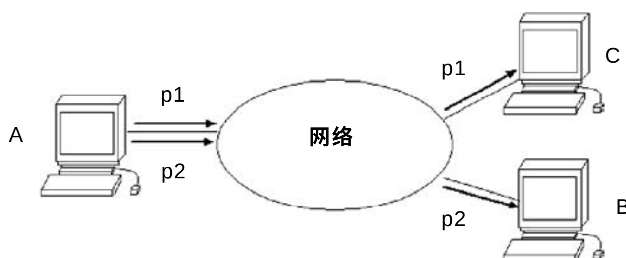


图7-2 组播应用

iSpirit 2924G/2924F交换机实现了IGMP，IGMP SNOOPING和二层静态组播，这些都是为组播应用服务。IGMP是组播组管理协议，由于iSpirit 2924G/2924F是二层交换机，没有实现直连子网内的三层IP组播地址的动态学习，但是可以发送query报文，维护组播组。IGMP SNOOPING监听网络上的IGMP包，实现IP组播MAC地址的动态学习。二层静态组播实现手工配置二层组播地址。

7.1 二层静态组播介绍

iSpirit 2924G/2924F交换机存在一个二层硬件组播转发表，可以实现二层组播的线速转发。组播MAC地址可以通过IGMP SNOOPING学习得到，也可以通过手工静态配置得到。

本节包括以下内容：

- 二层硬件组播转发表
- 二层组播MAC地址
- 二层组播转发模式
- 二层静态组播和二层动态组播

1.二层硬件组播转发表

二层硬件组播转发表实现二层组播流的线速转发，共有255个条目，可以容纳255个组播MAC地址。二层硬件组播转发表的每个条目有三个重要的字段，分别是：组播MAC地址、VLAN ID和输出端口列表，其中索引是组播MAC地址和VLAN ID号。

在二层硬件组播转发表中多个VLAN（也就是多个子网）可以存在相同的组播MAC地址，需要有多个条目来容纳。当二层组播流从交换机的一个端口输入时，首先得到二层组播流的组播MAC地址和所属的VLAN ID，查找二层硬件组播转发表，如果匹配了一个条目，把输出端口列表取出来，去除输入端口，二层组播流从这些端口发出去。输出端口列表中可以没有输出端口或只有一个输出端口或有多个输出端口。

2.二层组播 MAC 地址

MAC 地址分为组播 MAC 地址和单播 MAC 地址，组播 MAC 地址的最高字节的最低位为 1，单播 MAC 地址的最高字节的最低位为 0，如图 6-3 所示。例如地址 01:00:00:00:00:01 是组播 MAC 地址，地址 00:00:00:00:00:01 是单播 MAC 地址。

组播MAC地址

48	40	39 32	31 24	23 16	15 8	7 0
	1					

单播MAC地址

48	40	39 32	31 24	23 16	15 8	7 0
	0					

图 7-3 组播和单播 MAC 地址

组播 MAC 地址又分为 IP 组播 MAC 地址和非 IP 组播 MAC 地址。IP 组播 MAC 地址是三层 IP 组播地址映射成的组播 MAC 地址，其中前三个字节必须是 01:00:5e，第 23 位必须为 0，其它 23 位地址是三层 IP 组播地址的低 23 位映射而成。非 IP 组播 MAC 地址是除了 IP 组播 MAC 地址以外的所有组播 MAC 地址。例如 01:00:5e:00:00:01 是 IP 组播 MAC 地址，而 01:00:ff:00:00:01 是非 IP 组播 MAC 地址。如图 6-4 所示为 IP 组播 MAC 地址。

IP组播MAC地址

48 40	39 32	31 24	23	16	15 8	7 0
01	00	5e	0			

图 7-4 IP 组播 MAC 地址

3.二层组播转发模式

二层硬件组播转发表存在两种组播转发模式，分别是：未注册转发模式和注册转发模式。

对于未注册转发模式，当二层组播数据流从二层硬件组播转发表中找到匹配的条目，则根据该条目的输出端口列表进行转发，如果没有找到匹配的条目，则向该 VLAN 的所有其它端口转发，此时相当于广播。

对于注册转发模式，当二层组播数据流从二层硬件组播转发表中找到匹配的条目，则根据该条目的输出端口列表进行转发，如果没有找到匹配的条目，则丢弃该二层组播数据流。

iSpirit 2924G/2924F 交换机上如果 IGMP SNOOPING 是关闭的，二层组播处于未注册转发模式，如果 IGMP SNOOPING 是打开的，二层组播处于注册转发模式。

4.二层静态组播和二层动态组播

二层硬件组播转发表中的组 播 MAC 地址条目可以通过 IGMP SNOOPING 动态学习得到，也可以通过手工配置。通过 IGMP SNOOPING 动态学习到的是 IP 组播 MAC 地址，而通过手工配置的可以是 IP 组播 MAC 地址，也可以是非 IP 组播 MAC 地址。

当交换机关闭 IGMP SNOOPING 时，二层硬件组播转发表处于未注册转发模式，不能动态学习到组播 MAC 地址，二层硬件组播转发表中没有条目，所有的二层组播数据流当作广播处理。此时可以通过手工往二层硬件组播转发表中加静态组播条目，可以控制二层组播数据流只往指定的端口输出转发，减小网络的组播流量。

当网络具备组播环境时，为了有效控制网络的组播流量，交换机可以打开 IGMP SNOOPING，此时二层硬件组播转发表处于注册转发模式，交换机可以通过监听网络上的 IGMP 协议包学习到组播 MAC 地址，与二层硬件组播转发表中的条目匹配的二层组播流才能够转发。为了让学习不到的组播 MAC 地址的二层组播流得到转发，可以通过手工往二层硬件组播转发表中加静态组播条目。

当静态配置和动态学习到的 IP 组播 MAC 地址是二层硬件组播转发表中的同一个条目时，输出端口列表包括静态配置的端口和动态学习的端口。当删除静态配置的 IP 组播 MAC 地址时，只去除静态配置的端口，动态学习到的端口继续保留，当动态学习到的 IP 组播 MAC 地址不再存在时，只去除动态学习到的端口，静态配置的端口继续保留。

7.2 二层静态组播配置

iSpirit 2924G/2924F 交换机缺省情况下没有二层静态组播配置。本节描述二层静态组播的配置，主要包括以下内容：

- 配置二层组播地址
- 显示二层组播地址信息

1.配置二层组播地址

二层组播地址的配置非常简单，包括创建二层组播地址条目和增加二层组播地址条目的输出端口，删除二层组播地址条目和删除二层组播地址条目的输出端口。

- 下面的命令在全局 CONFIG 模式下创建二层组播地址条目和增加二层组播地址条目的输出端口，需要输入 VLAN ID、组播 MAC 地址和输出端口列表。如果该二层组播条目不存在，则创建一个二层组播条目，并把指定的端口列表当作该条目的输出端口列表。如果该二层组播条目存在，则把指定的端口列表增加到该条目的输出端口列表中。

multicast <vlanid> <mac-address> {<port>|<port1-port2>} [<port>|
<port1-port2>] …

- 下面的命令在全局 CONFIG 模式下删除二层组播地址条目和删除二层组播地址条目的输出端口，需要输入 VLAN ID 和组播 MAC 地址，端口可以输入也可以不输入。如果不输入端口，则删除此二层组播地址条目，该条目中所有的输出端口列表都被清除。如果输入端口，则从此二层组播地址条目的输出端口列表中去除指定的端口。

no multicast <vlanid> <mac-address> [<port>|<port1-port2>] …

2.显示二层组播地址信息

二层组播地址包括静态配置的二层组播地址和动态学习到的二层组播地址，iSpirit 2924G/2924F 交换机提供了两个二层组播地址的显示命令，一个显示静态配置的二层组播地址信息，另一个显示所有的二层组播地址信息，包括静态配置的和动态学习到的。

- 下面的命令在全局 CONFIG 模式下显示静态配置的二层组播地址信息：

show multicast static

- 下面的命令在全局 CONFIG 模式下显示所有的二层组播地址信息：

show multicast

7.3 二层静态组播配置示例

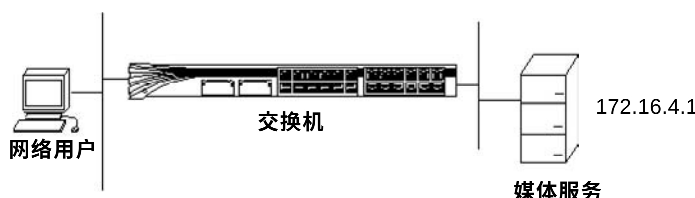


图 7-5 二层静态组播配置示例

例如有一个组播服务器 IP 地址为 172.16.4.1 ，在 VLAN2 内，发出组播服务的组播 IP 为 224.100.100.240，也就是而层组播 MAC 01:00:5e:64:64:f0

如果有用户 1 和用户 2 连接到 iSpirit 2924G/2924F 的 1 和 2 端口，并且需要组播服务的话，就需要在交换机上配置静态的组播组：

将端口 1-2 加入到组播 01:00:5e:64:64:f0（VLAN2）中：

```
 switch# multicast 2 01:00:5e:64:64:f0  1-2
Switch# show multicast static
multicast address:  01:00:5e:64:64:f0
vlan id:            2
port list:          1 2
```

第 8 章 配置 IGMP SNOOPING

本章对 IGMP SNOOPING **的概念和配置进行描述，主要包括以下内容：**

1、IGMP SNOOPING **介绍**

2、IGMP SNOOPING **配置**

在城域网/Internet 中，采用单播方式将相同的数据包发送给网络中的多个而不是全部接收者时，由于需要复制分组给每一个接收端点，随着接收者数量的增多，需要发出的包数也会线性增加，这使得主机、交换路由设备及网络带宽资源总体负担加重，效率受到极大影响。随着多点电视会议、视屏点播、群组通信应用等需求的增长，为提高资源利用率，组播方式日益成为多点通信中普遍采用的传输方式。

iSpirit 2924G/2924F 交换机实现了 IGMP，IGMP SNOOPING 和二层静态组播，这些都是为组播应用服务。IGMP 是组播组管理协议，实现直连子网内的三层 IP 组播地址的动态学习。IGMP SNOOPING 监听网络上的 IGMP 包，实现 IP 组播 MAC 地址的动态学习。二层静态组播实现手工配置二层组播地址。

8.1 IGMP SNOOPING 介绍

传统的网络在一个子网内组播数据包当作广播处理，这样容易使网络流量大，造成网络拥塞。当交换机上实现了 IGMP SNOOPING 后，IGMP SNOOPING 可以动态学习 IP 组播 MAC 地址，维护 IP 组播 MAC 地址的输出端口列表，使组播数据流只往输出端口发送，这样可以减少网络的流量。

二层静态组播是通过手工配置二层组播地址，而 IGMP SNOOPING 是通过动态学习二层组播地址，两者之间有密切的关系。二层静态组播请参见“配置二层静态组播”章节。本节主要包括以下内容：

- IGMP SNOOPING处理过程
- 二层动态组播和二层静态组播
- 加入一个组
- 离开一个组

1.IGMP SNOOPING处理过程

IGMP SNOOPING 是一个二层的网络协议，监听经过交换机的 IGMP 协议包，根据这些 IGMP 协议包的收包端口，vlanid，组播地址来维护一个组播组，然后转发这些 IGMP 协议包。只有加入了组播组的端口才可以接收组播数据流；这样就减少了网络的流量，节省了网络带宽。

组播组包括了组播组地址，成员端口，VlanId，Age，Type 字段。

IGMP SNOOPING 组播组的形成是一个学习的过程。当交换机的某一个端口收到 IGMP REPORT 包时，IGMP SNOOPING 会产生一个新的组播组，接收 IGMP REPORT 包的端口就被加入这个组播组。在交换机收到一个 IGMP QUERY 包时，如果这个组播组已经存在交换机中，那么这个收到 IGMP QUERY 的端口也加入到这个组播组中，否则只是转发 IGMP QUERY 包。IGMP SNOOPING 还支持 IGMP V2 的 Leave 机制；如果 IGMP SNOOPING 配置了 immediate leave 为 ENABLE，在收到 IGMP V2 的 leave 包时收包端口可以立刻离开组播组。

IGMP SNOOPING 有两种更新机制。一种是上面介绍的 leave 机制。大多数情况下 IGMP SNOOPING 是通过 age time 来删除过期的组播组的。当组播组加入 IGMP SNOOPING 时记录了加入的时间，当组播组在交换机中存留的时间超过了一个配置的 age time 时，交换机会删除这个组播组。

2.二层动态组播和二层静态组播

二层硬件组播转发表中的组播 MAC 地址条目可以通过 IGMP SNOOPING 动态学习得到，也可以通过手工配置。通过 IGMP SNOOPING 动态学习到的是 IP 组播 MAC 地址，而通过手工配置的可以是 IP 组播 MAC 地址，也可以是非 IP 组播 MAC 地址。

当交换机关闭 IGMP SNOOPING 时，二层硬件组播转发表处于未注册转发模式，不能动态学习到组播 MAC 地址，二层硬件组播转发表中没有条目，所有的二层组播数据流当作广播处理。此时可以通过手工往二层硬件组播转发表中加静态组播条目，可以控制二层组播数据流只往指定的端口输出转发，减小网络的组播流量。

当网络具备组播环境时，为了有效控制网络的组播流量，交换机可以打开 IGMP SNOOPING，此时二层硬件组播转发表处于注册转发模式，交换机可以通过监听网络上的 IGMP 协议包学习到组播 MAC 地址，与二层硬件组播转发表中的条目匹配的二层组播流才能够转发。为了让学习不到的组播 MAC 地址的二层组播流得到转发，可以通过手工往二层硬件组播转发表中加静态组播条目。

当静态配置和动态学习到的 IP 组播 MAC 地址是二层硬件组播转发表中的同一个条目时，输出端口列表包括静态配置的端口和动态学习的端口。当删除静态配置的 IP 组播 MAC 地址时，只去除静态配置的端口，动态学习到的端口继续保留，当动态学习到的 IP 组播 MAC 地址不再存在时，只去除动态学习到的端口，静态配置的端口继续保留。

3.加入一个组

当一个主机想加入一个组播组时，主机会发一个 IGMP REPORT 包，在此包中指定主机要加入的组播组。当交换机收到一个 IGMP QUERY 包时，交换机会把该包转发给同一个 VLAN 的所有其它端口，当端口下想加入组播组的主机收到 IGMP QUERY 包后会回送一个 IGMP REPORT 包。当交换机收到一个 IGMP REPORT 包后，会建立一个二层组播条目，收到 IGMP QUERY 包的端口和 IGMP REPORT 包的端口会加入到该二层组播条目，成为它的输出端口。

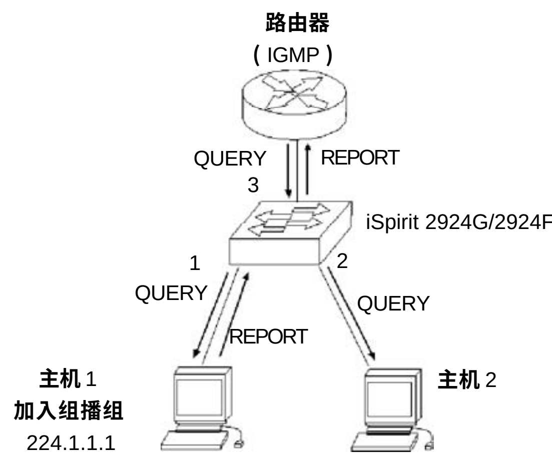


图 8-1 主机 1 加入组播组

如上图 8-1 所有的设备在一个子网内，假设该子网的 VLAN 是 2。产品运行 IGMPv2 协议，定时发送 IGMP QUERY 包。主机 1 想加入组播组 224.1.1.1。交换机从 3 端口收到 IGMP QUERY 包后会记录此端口并把该包转发给端口 1 和 2。主机 1 收到 IGMP QUERY 包后回送一个 IGMP REPORT 包，主机 2 因为不想加入组播组，不发 IGMP REPORT 包。交换机从端口 1 收到 IGMP REPORT 包后会把该包从查询端口 3/1 转发出去并且创建一个二层组播条目（假定该条目不存在），该二层组播条目包括以下几项：

表 8-1：

二层组播地址	vlan ID	输出端口列表
01:00:5e:01:01:01	2	1，3

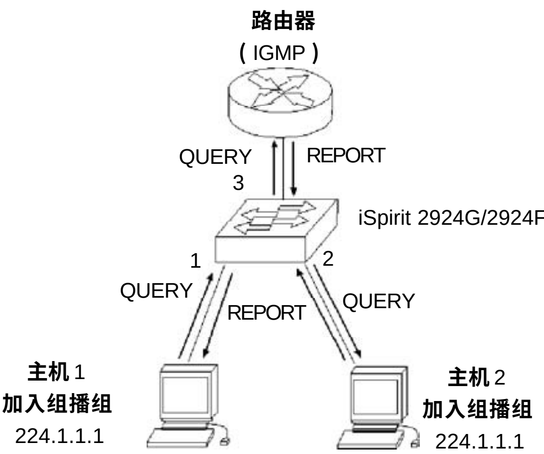


图 8-2 主机 1 和主机 2 加入组播组

如图 8-2 的条件与图 8-1 一样，主机 1 已经加入了组播组 224.1.1.1，现在图 7-2 中的主机 2 想加入组播组 224.1.1.1。当主机 2 收到 IGMP QUERY 包后回送一个 IGMP REPORT 包，交换机从端口 2 收到 IGMP REPORT 后会把该包从查询端口 3 转发出去并且会包端口 2 加入到二层组播条目中，该二层组播条目变为：

表 8-2：

二层组播地址	vlan ID	输出端口列表
01:00:5e:01:01:01	2	1 ,2, 3

4.离开一个组

为了能够组成一个稳定的组播环境，运行 IGMP 的设备（如路由器）会每隔一定的时间发送一个 IGMP QUERY 包给所有的主机。已经加入组播组或想加入组播组的主机收到该 IGMP QUERY 后会回送一个 IGMP REPORT。

如果主机想离开一个组播组，可以有两种方式：主动离开和被动离开。主动离开就是主机发送一个 IGMP LEAVE 包给路由器，被动离开就是当主机收到路由器发来的 IGMP QUERY 后不回送 IGMP REPORT。

与主机离开组播组的方式对应，在交换机上端口脱离二层组播条目的方式也有两种：超时离开和收到 IGMP LEAVE 包离开。

当交换机超过一定的时间没有从一个端口收到一个组播组的 IGMP REPORT 包时，该端口要从对应的二层组播条目中清除，如果该二层组播条目没有了端口，则删除此二层组播条目。

当交换机的 immediate leave 配置为 ENABLE 时，如果某个端口收到一个组播组的 IGMP LEAVE 包时，该端口从对应的二层组播条目中清除，如果该二层组播条目没有了端口，则删除此二层组播条目。immediate leave 一般应用在一个端口下接一个主机的情况。

8.2 IGMP SNOOPING 配置

本节介绍 IGMP SNOOPING 的配置，主要包括以下内容：

- IGMP SNOOPING缺省配置
- 打开和关闭IGMP SNOOPING
- 打开和关闭 immediate leave
- 配置组播组 age 时间
- 显示组播组信息

1. IGMP SNOOPING缺省配置

IGMP SNOOPING 缺省是关闭的，二层硬件组播转发表处于未注册转发模式。

immediate leave 缺省是关闭的。

组播组 age 时间缺省为 300 秒。

2.打开和关闭IGMP SNOOPING

下面的命令在全局 CONFIG 模式下打开 IGMP SNOOPING，会往所有端口的 FFP 中加一个条目：

igmp snooping

下面的命令在全局 CONFIG 模式下关闭 IGMP SNOOPING：

no igmp snooping

3.打开和关闭 immediate leave

- 下面的命令在全局 CONFIG 模式下打开 immediate leave：

  igmp snooping immediate-leave
- 下面的命令在全局 CONFIG 模式下关闭 immediate leave：

  no igmp snooping immediate-leave

4.配置组播组 age 时间

下面的命令在全局 CONFIG 模式下设置组播组的 age 时间，单位为秒

igmp snooping age <age-interval>

5.显示组播组信息

- **下面的命令在全局** CONFIG **模式下显示** IGMP SNOOPING **的所有信息：**

show igmp snooping

- **下面的命令在全局** CONFIG **模式下显示所有的二层组播组的信息，包括** IGMP SNOOPING **学习到的和静态配置的二层组播条目：**

show multicast

第 9 章 配置 AAA

本章描述如何配置 iSpirit 2924G/2924F **交换机的** 802.1x **和** RADIUS **以防止非法用户接入网络。关于** 802.1x **客户端和** HyperBoss **的使用请参见各自的操作手册。本章主要包括以下内容：**

1、802.1x **介绍**
2、RADIUS **介绍**
3、**配置** 802.1x
4、**配置** 802.1x **配置实例**
5、**配置** RADIUS

AAA 是认证，授权和计费（Authentication, Authorization, and Accounting）的简称。它提供了一个用来对认证，授权和计费这三种安全功能进行配置的一致的框架。AAA 的配置实际上是对网络安全的一种管理，这里的网络安全主要指访问控制。包括哪些用户可以访问网络？具有访问权的用户可以得到哪些服务？如何对正在使用网络资源的用户进行记账？

- 认证(Authentication): 验证用户是否可以获得访问权。
- 授权(Authorization)：授权用户可以使用哪些服务。
- 计费(Accounting)：记录用户使用网络资源的情况。

联想网络公司推出了一整套 AAA 的解决方案，产品有 802.1x 客户端、各种支持认证的交换机和认证计费系统 HyperBoss。802.1x 客户端安装在用户上网的 PC 机上，当用户需要访问网络时，需要使用 802.1x 客户端进行认证，只有通过认证的用户才能使用网络。iSpirit 2924G/2924F 是一款支持认证的交换机，它接收客户端的认证请求，把用户名和口令传送给认证计费系统 HyperBoss，交换机本身不做实际的认证工作。HyperBoss 接收交换机发来的认证请求进行实际的认证，并对认证成功的用户进行计费处理。

在 802.1x 客户端和交换机之间使用 802.1x 协议进行通信，在交换机和 HyperBoss 之间使用 RADIUS 协议进行通 信 。

9.1 802.1x 介绍

802.1x 协议是一个基于端口的访问控制和认证协议，这里指的端口是逻辑端口，可以是物理端口、MAC 地址或 Vlan ID 等，联想网络的交换机实现的都是基于 MAC 地址的 802.1x 协议。

802.1x 是一个二层协议，认证的交换机和用户的 PC 机必须处于同一个子网中，协议包不能跨越网段。802.1x 认证采用的是客户服务器的模型，必须有一个服务器对所有的用户进行认证。在用户通过认证之前，只有认证流能够通过交换机的端口，在认证成功后，数据流才能通过交换机的端口，也就是说用户必须在认证通过后才能访问网络。

本节主要包括以下内容：

- 802.1x 设备组成
- 协议包简介
- 协议流交互
- 802.1x 端口状态

1. 802.1x 设备组成

802.1x 设备由三部分组成：客户端（Supplicant System）、认证系统（Authenticator System）和认证服务器（Authentication Server System）。如图 9-1 所示。

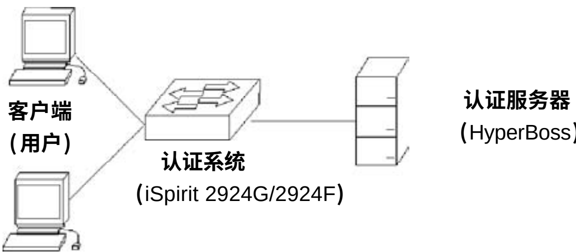


图 9-1 802.1x 设备

客户端指的是请求访问网络的设备，一般是用户终端系统，如用户的 PC 机，在用户终端系统上必须要安装一个 802.1x 客户端软件，该软件实现 802.1x 协议中的客户端部分。

客户端发起 802.1x 认证请求，请求认证服务器对其用户名和口令进行验证，如果认证成功，用户可以访问网络。

认证系统指的是认证的设备，如 iSpirit 2924G/2924F 交换机。认证系统通过用户的逻辑端口（指的是 MAC 地址）的状态控制用户是否可以访问网络，如果用户的逻辑端口状态是非授权的，则用户不可以访问网络，如果用户的逻辑端口状态是授权的，则用户可以访问网络。

认证系统是客户端和认证服务器之间的一个中继。认证系统请求用户的身份信息，并把用户的身份信息转发

给认证服务器，并把认证服务器发来的认证结果转发给客户端。认证系统在靠近用户端要实现 802.1x 协议的服务端部分，在靠近认证服务器端要实现 RADIUS 协议的客户端部分，认证系统的 RADIUS 协议客户端把 802.1x 客户端送来 EAP 信息封装在 RADIUS 中发送给认证服务器，并从认证服务器发来的 RAIDUS 协议包中把 EAP 信息解封装出来并通过 802.1x 服务端部分传送给 802.1x 客户端。

认证服务器指的是实际对用户进行认证的设备。认证服务器接收认证系统发来的用户的身份信息并进行验证，如果认证成功，认证服务器对认证系统进行授权，允许用户访问网络，如果认证失败，认证服务器告诉认证系统用户认证失败，用户不能访问网络。认证服务器和认证系统之间通过 EAP 扩展的 RADIUS 协议进行通信。联想网络提供了认证计费系统 HyperBoss 对用户进行认证和计费。

2.协议包简介

802.1x 协议在网络上传输的认证数据流是 EAPOL（EAP Over LAN）帧格式，所有的用户身份信息（包括用户名和口令）封装在 EAP（扩展认证协议）中，EAP 再封装在 EAPOL 帧中。用户名以明文的形式在 EAP 中存在，而口令则以 MD5 加密的形式在 EAP 中存在。

EAPOL 帧格式如图 9-2。PAE Ethernet Type 是 EAPOL 的以太网协议类型号，值为 0x888E。Protocol Version 是 EAPOL 版本号，值为 1。Packet Type 指的是 EAPOL 帧类型。Packet Body Length 是 EAPOL 帧内容的长度。Packet Body 指的是 EAPOL 帧的内容。

Field	Octet Number
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

图 9-2 EAPOL 帧格式

联想交换机使用了三种 EAPOL 协议帧，分别是：

EAPOL-Start：Packet Type 的值为 1，认证发起帧，当用户需进行认证时首先发起此帧，由客户端发给交换机。

EAPOL-Logoff：Packet Type 的值为 2，退出请求帧，当用户不需要使用网络时发此帧通知交换机。

EAP-Packet：Packet Type 的值为 0，认证信息帧，用于承载认证信息。

EAP 包格式如图 9-3。Code 指的是 EAP 包的类型，包括 Request、Response、Success 和 Failure。Identifier 指的是标识符，用于匹配 Response 和 Request。Length 指的是 EAP 包长度，包括包头。Data 指的是 EAP 包数据。

EAP 包包括以下四种类型：

EAP-Request：Code 值为 1，EAP 请求包，从交换机发给客户端请求用户名和（或）口令。

EAP-Response：Code 值为 2，EAP 应答包，从客户端发给交换机，把用户名和（或）口令送给交换机。

EAP-Success：Code 值为 3，EAP 成功包，从交换机发给客户端，告诉客户端用户认证成功。

EAP-Failure：Code 值为 4，EAP 失败包，从交换机发给客户端，告诉客户端用户认证失败。

Field	Octet Number
Code	1
Identifier	2
Length	3-4
Data	5-N

图 9-3 EAP 包格式

3.协议流交互

当交换机使能 802.1x 并且端口的状态是 Auto 时，该端口下的所有接入用户都必须通过认证后才能访问网络。协议交互如图 9-4。

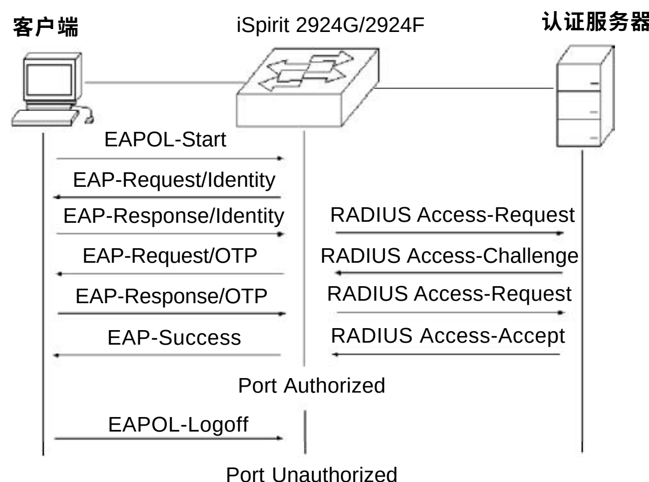


图 9-4　客户端发起认证的协议交互

当用户需要访问网络时，客户端首先发送 EAPOL-Start 给交换机请求认证，交换机收到认证请求后发送 EAP-Request 请求用户的用户名，客户端回送 EAP-Response，交换机把 EAP 信息提取出来封装在 RADIUS 包中发给认证服务器，认证服务器请求用户的口令，交换机发送 EAP-Request 给客户端请求用户的口令，客户端回送 EAP-Response，交换机把 EAP 信息封装在 RADIUS 包中发送给认证服务器，认证服务器根据用户名和口令对用户进行认证。如果认证成功，认证服务器通知交换机，交换机发 EAP-Success 给客户端并把用户的逻辑端口处于授权状态。当客户端收到 EAP-Success 后表示认证成功，用户可以访问网络。

当用户不再需要使用网络，客户端发送 EAPOL-Logoff 给交换机，交换机把用户的逻辑端口状态迁为非授权状态，此时用户不能访问网络。

为了防止客户端异常下线，iSpirit 2924G/2924F 交换机提供了重新认证的机制，可以在交换机上设定重新认证的间隔时间，当认证时间到达，交换机发起重新认证，如果认证成功，用户可以继续使用网络，如果认证失败，用户将不能使用网络。协议交互如图 9-5。

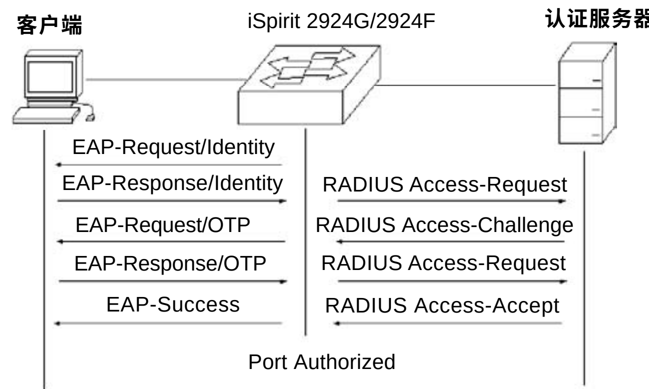


图 9-5　重新认证的协议交互

4. 802.1x 端口状态

这里指的端口状态是交换机的物理端口状态。交换机的物理端口存在四种状态：N/A 状态、Auto 状态、Force-authorized 状态和 Force-unauthorized 状态。当交换机没有打开 802.1x 时，所有的端口处于 N/A 状态。当交换机端口要设置成 Auto 状态、Force-authorized 状态或 Force-unauthorized 状态时，必须先使能交换机的 802.1x。

当交换机的端口处于 N/A 状态时，端口下的所有用户不需要认证就可以访问网络。当交换机从该端口收到 802.

1x 协议包时，丢弃这些协议包。

当交换机的端口处于 Force-authorized 状态时，端口下的所有用户不需要认证就可以访问网络。当交换机从该端口收到 EAPOL-Start 包时，交换机回送 EAP-Success 包，当交换机从该端口收到其它的 802.1x 协议包时，丢弃这些协议包。

当交换机的端口处于 Force-unauthorized 状态时，端口下的所有用户始终不能访问网络，认证请求永远通不过。当交换机从该端口收到 802.1x 协议包时，丢弃这些协议包。

当交换机的端口处于 Auto 状态时，端口下的所有用户必须通过认证后才能访问网络。802.1x 协议交互如图 9-4。如果用户需要做认证，端口一般要设置成 Auto 状态。

9.2 RADIUS 介绍

当用户进行认证时，交换机和认证服务器之间采用支持 EAP 扩展的 RADIUS 协议进行交互。RADIUS 协议采用客户 / 服务器模型，交换机需要实现 RADIUS 客户端，而认证服务器需要实现 RADIUS 服务端。

为了保证交换机和认证服务器之间交互的安全性，防止非法的交换机或非法的认证服务器之间的交互，交换机和认证服务器之间要相互鉴权。交换机和认证服务器需要一个相同的密钥，当交换机或认证服务器发送 RADIUS 协议包时，所有的协议包要根据密钥采用 HMAC 算法生成消息摘要，当交换机和认证服务器收到 RADIUS 协议包时，所有的协议包的消息摘要要使用密钥进行验证，如果验证通过，认为是合法的 RADIUS 协议包，否则是非法的 RADIUS 协议包，将丢弃非法的 RADIUS 协议包。

本节主要包括以下内容：

●协议包简介

●协议流交互

●用户验证方法

1.协议包简介

RADIUS 是建立在 UDP 之上的协议，RADIUS 可以封装认证信息和计费信息。早期的 RADIUS 认证端口是 1645，目前使用端口 1812，早期的 RADIUS 计费端口是 1646，目前使用端口 1813。

因为 RADIUS 承载在 UDP 上， 所以 RADIUS 要有超时重发机制。同时为了提高认证系统与 RADIUS 服务器通信的可靠性，一般采用两个 RADIUS 服务器方案，即采用备用服务器机制。

RADIUS 报文格式如图 9-6。Code 指 RADIUS 协议报文类型。Identifier 指标识符，用于匹配请求和应答。Length 指整个报文（包括报文头）的长度。Authenticator 是一个 16 字节的串，对于请求包是一个随机数，对于应答包是 MD5 生成的消息摘要。Attribute 指 RADIUS 协议包中的属性。

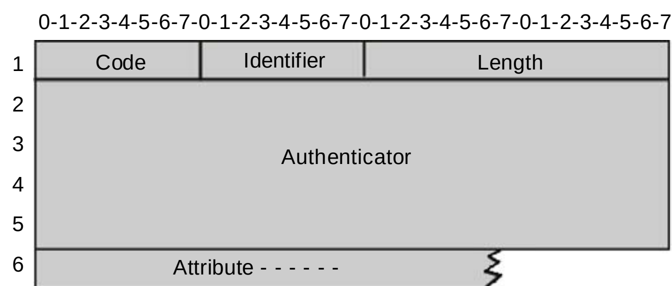


图 9-6 RADIUS 报文格式

联想网络使用了以下几种 RADIUS 协议包：

● Access-Request：Code 值为 1，从认证系统发给认证服务器的认证请求包，用户名和口令封装在此包上。

● Access-Accept：Code 值为 2，从认证服务器发给认证系统的应答包，表示用户认证成功。

● Access-Reject：Code 值为 3，从认证服务器发给认证系统的应答包，表示用户认证失败。

● Access-Challenge：Code 值 11，从认证服务器发给认证系统的应答包，表示认证服务器需要用户的进一步的信息，如口令等。

● Accounting-Request：Code 值为 4，从认证系统发给认证服务器的计费请求包，包括开始计费和结束计费

包，计费信息封装在此包上。

●Accounting-Response：Code 值为 5，从认证服务器发给认证系统的计费应答包，表示计费信息已收到。

2.协议流交互

当用户发起认证后认证系统和认证服务器之间通过 RADIUS 协议进行交互。认证系统不发 RADIUS 计费包的协议流交互如图 9-4。一般情况下，在用户认证成功后或用户下线时，认证系统需要给认证服务器发 RADIUS 计费包，协议流交互如图 9-7 所示。

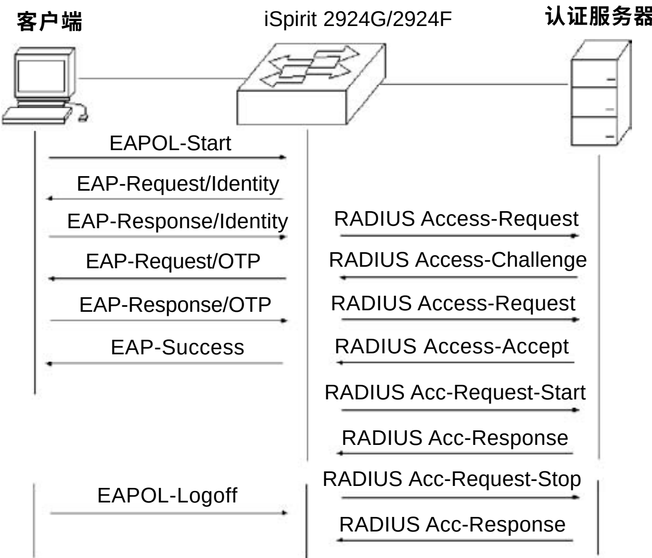


图 9-7 协议流交互

用户进行认证时，交换机把用户名封装在 Access-Request 报文中发给认证服务器，服务器应答 Access-Challenge 请求用户的口令，交换机请求客户端用户的口令，客户端把口令封装在 EAP 中，交换机获取到此 EAP 后封装在 Access-Request 发给认证服务器，认证服务器对用户进行认证，如果认证成功，回送 Access-Accept 给交换机，交换机收到此报文后通知客户端认证成功，同时发送 Accounting-Request 通知认证服务器开始计费，认证服务器回送 Accounting-Response。

当用户不想使用网络时，通知交换机用户下线，交换机发 Accounting-Request 通知认证服务器结束计费，计费信息封装在此包中，认证服务器回送 Accounting-Response。

3.用户验证方法

RADIUS 有三种用户验证方法，如下：

PAP（Password Authentication Protocol)。用户以明文的形式把用户名和他的密码传递给交换机。 交换机通过 RADIUS 协议包把用户名和密码传递给 RADIUS 服务器，RADIUS 服务器查找数据库，如果存在相同的用户名和密码表明验证通过,否则表明验证未通过。

CHAP（Challenge Handshake Authentication Protocol)。当用户请求上网时，交换机产生一个 16 字节的随机码给用户。用户对随机码，密码以及其它各域加密生成一个 response，把用户名和 response 传给交换机。交换机把用户名，response 以及原来的 16 字节随机码传给 RADIUS 服务器。RADIU 根据用户名在交换机端查找数据库，得到和用户端进行加密所用的一样的密码，然后根据传来的 16 字节的随机码进行加密，将其结果与传来的 response 作比较，如果相同表明验证通过，如果不相同表明验证失败。

EAP（Extensible Authentication Protocol)。用此种验证方法，交换机并不真正参与验证，只起到用户和 RADIUS 服务器之间的转发作用。当用户请求上网时，交换机请求用户的用户名，并把用户名转送给 RADIUS 服务器，RADIUS 服务器产生一个 16 字节的随机码给用户并存储该随机码，用户对随机码，密码以及其它各域加密生成一个 response，把用户名和 response 传给交换机，交换机转发给 RADIUS 服务器。 RADIU 根据用户名在交换机端查找数据库，得到和用户端进行加密所用的一样的密码，然后根据存储的 16 字节的随机码进行加密，将

其结果与传来的 response 作比较，如果相同表明验证通过，如果不相同表明验证失败。

联想网络的认证计费解决方案采用的是 EAP 用户验证方法。

9.3 配置 802.1x

本节对 802.1x 的配置进行详细的描述，主要包括以下内容：

●802.1x 缺省配置

●启动和关闭 802.1x

●配置 802.1x 端口状态

●配置重新认证机制

●配置端口接入主机最大个数

●配置间隔时间和重发次数

●显示 802.1x 信息

1. 802.1x 缺省配置

iSpirit 2924G/2924F 交换机 802.1x 配置缺省情况如下：

● 802.1x 是关闭的

● 所有端口的状态是 N/A

● 重新认证机制是关闭的，重新认证的间隔时间是 3600 秒

● 所有端口的接入主机最大个数是 9 个

● 重发 EAP-Request 的超时间隔为 30 秒

● 超时重发 EAP-Request 的次数为 3 次

● 用户认证失败等待的时间为 60 秒

● 服务端超时重发的时间间隔为 10 秒

交换机在全局 CONFIG 模式下提供一个命令让所有的配置回到缺省状态，命令如下：

dot1x default

2.启动和关闭 802.1x

●配置 802.1x 的第一步是启动 802.1x。在全局 CONFIG 模式下输入下面的命令启动 802.1x：

dot1x

●当关闭 802.1x 时，所有的端口状态回到 N/A 状态。在全局 CONFIG 模式下输入下面的命令关闭 802.1x：

no dot1x

3.配置 802.1x 端口状态

在设置 802.1x 端口状态前一定要启动 802.1x。如果端口下的所有的用户必须通过认证后才能访问网络，则该端口必须设置成 Auto 状态。

●下面的命令在全局 CONFIG 模式下设置端口为 Auto 状态：

dot1x control auto <port number>

●下面的命令在 PORT RANGE 模式下设置端口为 Auto 状态：

dot1x control auto

●下面的命令在全局 CONFIG 模式下设置端口为 Force-authorized 状态：

dot1x control force-authorized <port number>

●下面的命令在 PORT RANGE 模式下设置端口为 Force-authorized 状态：

dot1x control force-authorized

●下面的命令在全局 CONFIG 模式下设置端口为 Force-unauthorized 状态：

dot1x control force-unauthorized <port number>

●下面的命令在 PORT RANGE 模式下设置端口为 Force-unauthorized 状态：

dot1x control force-unauthorized

●下面的命令在全局 CONFIG 模式下设置端口为 N/A 状态：

no dot1x control <port number>

●下面的命令在 PORT RANGE 模式下设置端口为 N/A 状态：

no dot1x control

注 意 ：

若一端口已经绑定了 MAC 地址，则这个端口不能设置为 Auto、Force-authorized 或 Force-unauthorized 状态。

4.配置重新认证机制

为了防止客户端异常下线后交换机和认证服务器无法察觉，iSpirit 2924G/2924F 交换机提供了重新认证机制，每隔重新认证间隔时间交换机发起一次认证。

●下面的命令在全局 CONFIG 模式下启动重新认证机制：

dot1x reauthenticate

●下面的命令在全局 CONFIG 模式下关闭重新认证机制：

no dot1x reauthenticate

●下面的命令在全局 CONFIG 模式下设置重新认证的间隔时间：

dot1x timeout re-authperiod <interval>

注 意 ：

重新认证的间隔时间不要设置太短，否则网络带宽以及交换机的 CPU 资源消耗太大。

5.配置端口接入主机最大个数

iSpirit 2924G/2924F 交换机的每个端口都可控制接入的最大主机个数，此功能可以限制用户使用多台主机非法接入到网络中。端口接入主机最大个数缺省是 100 个，最大可以设置成 100 个。如果端口的接入主机最大个数设置为 0，那么该端口拒绝任何用户接入。

下面的命令在全局 PORT RANGE 模式下设置端口接入主机最大个数：

dot1x support-host <number>

6.配置间隔时间和重发次数

802.1x 协议标准中规定了协议交互和协议状态机的一些间隔时间和重发次数，iSpirit 2924G/2924F 交换机使用了标准的间隔时间和重发次数，建议用户在使用时不要改这些间隔时间和重发次数。

tx-period 表示交换机重发 EAP-Request 协议包的间隔时间；max-req 表示交换机重发 EAP-Request 的次数；quiet-period 表示用户认证失败时等待用于重新认证的间隔时间；server-timeout 表示交换机给认证服务器重发 RADIUS 包的间隔时间。

下面的命令在全局 CONFIG 模式下配置这些间隔时间和重发次数：

dot1x timeout tx-period <interval>

dot1x max-req <number>

dot1x timeout quiet-period <interval>

dot1x timeout server-timeout <interval>

7.显示 802.1x 信息

下面的命令在全局 CONFIG 模式或 PORT RANGE 模式下显示 802.1x 的信息，当不输入端口参数，显示所有的 802.1x 配置信息，包括所有端口的配置信息，当输入端口参数，显示该端口下的所有接入用户的信息：

show dot1x [m/p]

9.4 802.1X配置实例

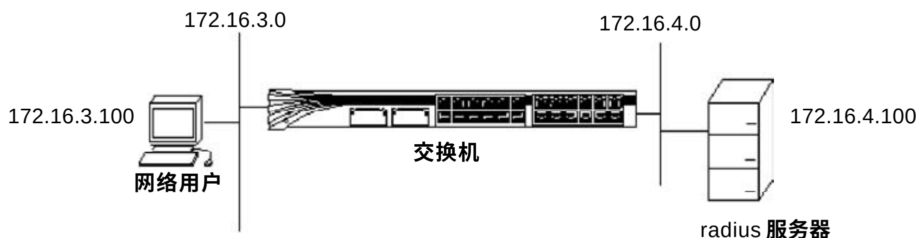


图 9-8 802.1X 配置实例

2924G/2924F 交换机划分了两个 vlan，vlan 1 是放置了 radius 服务器，ip 网段为 172.16.4.0，子网掩码为 255.255.255.0，2924G/2924F 上的 vlan1 子网接口 ip 为 172.16.4.1，radius 服务器的 ip 地址为 172.16.4.100。另一个 vlan2 为网络用户使用的 vlan，ip 网段为 172.16.3.0，子网掩码为 255.255.255.0，vlan2 的子网接口为 172.16.3.1，有一用户的 ip 地址为 172.16.3.100 并且联接到 2924G/2924F 交换机的第 1 端口。为了控制非法用户使用网络，需要在 2924G/2924F 交换机上打开 802.1x 认证机制，在用户使用的 pc 机上安装 802.1x 客户端，用户只有输入正确的用户名和密码并通过 radius 服务器认证，才能访问网络，用户的数据才能被交换机进行路由和转发。

整体打开 2924G/2924F 的 802.1x 的认证进程，

Switch# dot1x

打开特定端口为 802.1x 的认证端口，实例为 2924G/2924F 交换机的 1 端口

Switch# dot1x control auto 1

为 2924G/2924F 交换机指定 radius 服务器的 ip 地址

Switch# radius host 172.16.4.100

配置和 radius 服务器相匹配的认证密匙。根据实际情况要和 radius 所配置的一致

Switch# radius key rad123

查看 802.1x 是否配置正确

```
Switch# show dot1x
 Global 802.1X Parameters
 Dot1x Status          :     Enable
 ReAuth-enabled        :     no
 Accounting-enabled    :     yes
 ReAuth-period         :     3600
 Quiet-period          :     60
 Tx-period             :     30
 Supp-timeout          :     30
 Server-timeout        :     10
 Max-req               :     3
 reAuthMax             :     3

 802.1X Port Summary
 PortName   Status      Mode      HostNum
  1         Link Down   auto      100
  2         Link Down   n/a       100
  3         Link Down   n/a       100
```

查看 1 端口的状态

```
Switch# show dot1x 1
 Port-control         : auto
 Maximum hosts        : 100
```

Current Connecting hosts : 0

查看所配置的 radius **服务器是否正确**
Switch# show radius-server
PrimaryServerIp : 172.16.4.100
OptionServerIp : 0.0.0.0
UdpPort : 1812
accountingPort : 1813
ShareKey : rad123
Vendor :
NasPort : 0xc353
NasPortType : 0x0f
NasPortServer : 0x02

排 错 ：
1、**确认一定要打开** 802.1x **的认证进程，用** show dot1x **命令**
2、**确认打开特定的交换机端口做为认证端口，用** show dot1x **端口号**
3、**正确配置** radius **服务器的** ip **地址，用** show radius-server **命令查看**
4、**确认** radius **服务器和交换机之间所配置的认证密匙要一致**

9.5 配置 RADIUS

本节对 RADIUS **的配置进行详细的描述，主要包括以下内容：**
● RADIUS **缺省配置**
●**配置认证服务器的** IP **地址**
●**配置共享密钥**
●**启动和关闭计费**
●**配置** RADIUS **端口和属性信息**
●**显示** RADIUS **信息**

1.RADIUS缺省配置

iSpirit 2924G/2924F **交换机** RADIUS **配置缺省情况如下：**
没有配置主认证服务器和备份认证服务器的 IP **地址，也就是** IP **地址是** 0.0.0.0。
没有配置共享密钥，也就是共享密钥字符串为空。
计费缺省是启动的。
RADIUS **认证** UDP **端口为** 1812，**计费** UDP **端口为** 1813。
RADIUS **属性** NASPort **的值为** 0xc353，NASPortType **的值为** 0x0f，NASPortServer **的值为** 0x02。

2.配置认证服务器的 IP 地址

为了使交换机与认证服务器之间进行 RADIUS **通信，在交换机上需要配置认证服务器的** IP **地址。在实际应用中，可以使用一台认证服务器，也可以使用两台认证服务器，一台作为主认证服务器，一台作为备份认证服务器。如果交换机配置了两台认证服务器的** IP **地址，当交换机与主认证服务器中断通信后可以切换到与备份认证服务器通信。**

●**下面的命令在全局** CONFIG **模式下配置主认证服务器的** IP **地址：**
radius-server host <ip-address>
●**下面的命令在全局** CONFIG **模式下配置备份认证服务器的** IP **地址：**
radius-server option-host <ip-address>

3.配置共享密钥

交换机和认证服务器之间要相互鉴权，交换机和认证服务器上都需要设置一个相同的共享密钥。注意交换机

上的共享密钥一定要和认证服务器的相同。

下面的命令在全局 CONFIG **模式下配置交换机的共享密钥：**

radius-server key <string>

4.启动和关闭计费

如果交换机关闭了计费，交换机在认证成功后或用户下线时不会给认证服务器发 RADIUS **计费包。一般在实际应用时，计费是打开的。**

- **下面的命令在全局** CONFIG **模式下启动计费：**
  radius-server accounting
- **下面的命令在全局** CONFIG **模式下关闭计费：**
  no radius-server accounting

5.配置 RADIUS 端口和属性信息

建议用户不要修改 RADIUS **端口和属性信息配置。**

- **下面的命令在全局** CONFIG **模式下修改** RADIUS **认证** UDP **端口：**
  radius-server udp-port <port-number>
- **下面的命令在全局** CONFIG **模式下修改** RADIUS **属性信息：**
  radius-server attribute nas-portnum <number>
  radius-server attribute nas-porttype <number>
  radius-server attribute service-type <number>

6.显示 RADIUS 信息

下面的命令在全局 CONFIG **模式下显示** RADIUS **配置信息：**

show radius-server

第 10 章 配置 MAC 绑定

在实际的网络中，用户的接入安全是管理员非常关注的问题。iSpirit 2924G/2924F 交换机提供了多种方式实现了用户的接入安全，其中就包括 MAC 绑定方式。本章介绍如何配置 MAC 绑定功能，主要包括以下内容：

1、MAC 绑定介绍

2、MAC 绑定配置

3、MAC 绑定配置示例

10.1 MAC 绑定介绍

MAC 绑定可以实现网络中的用户的接入安全。用户是通过交换机的端口接入到网络。如果交换机中的某端口绑定了特定的 MAC 地址，那么这些特定的 MAC 地址就是合法的 MAC 地址，交换机允许这些合法的 MAC 地址的用户从该端口接入网络，不允许非法的 MAC 地址的用户接入网络，实现用户的接入安全。

如果交换机的某端口绑定了 MAC 地址，交换机会一直检查从该端口输入的数据流，如果数据流的源 MAC 地址是被绑定的合法的 MAC 地址，该数据流允许转发，如果数据流的源 MAC 地址不是被绑定的合法的 MAC 地址，该数据流丢弃。通过丢弃输入的数据流来防止非法用户接入网络。

IEEE802.1Q 标准支持 SVL 和 IVL 两种 MAC 地址学习模式。SVL 指 MAC 地址与 VLAN 没有关系，在所有的 VLAN 中 MAC 地址必须唯一，在学习 MAC 地址时不关心 VLAN。IVL 指 MAC 地址与 VLAN 有关系，在不同的 VLAN 中 MAC 地址可以相同，但在一个 VLAN 内 MAC 地址必须唯一，在学习 MAC 地址时必须知道该 MAC 地址所属的 VLAN。iSpirit 2924G/2924F 交换机支持 IVL 模式，在做 MAC 绑定时必须指定这些 MAC 地址所属的 VLAN。

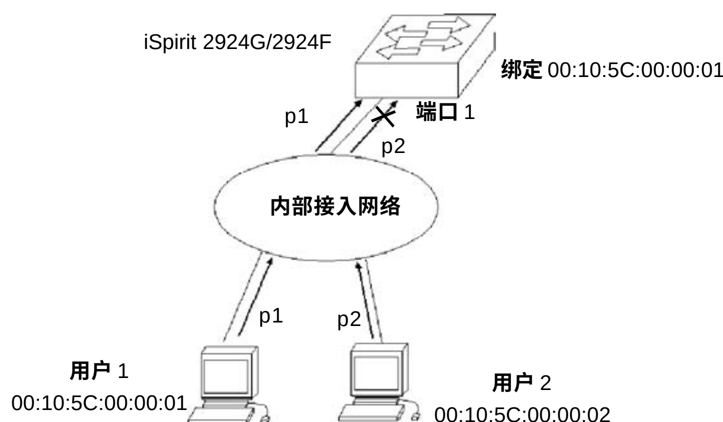


图 10-1 用户从绑定的端口接入网络

图 10-1 是一个 MAC 绑定的例子，iSpirit 2924G/2924F 交换机的端口 1 绑定了 MAC 地址 00:10:5C:00:00:01，在该端口下，有两个用户想从该端口接入网络，用户 1 的 MAC 地址是 00:10:5C:00:00:01，用户 2 的 MAC 地址是 00:10:5C:00:00:02。用户 1、用户 2 和交换机的端口 1 属于一个子网。只有用户 1 可以通过交换机的端口 1 接入网络，用户 2 不能通过交换机的端口 1 接入网络。用户 1 发出来的数据流 p1 可以通过交换机的端口 1 转发，而用户 2 发出来的数据流 p2 则在交换机的端口 1 处丢弃。

当交换机的某端口绑定了 MAC 地址时，这些 MAC 地址只能通过此交换机的该端口访问网络，不能通过该交换机的其它端口访问网络。交换机的不同端口不能绑定相同的 VLAN 的相同的 MAC 地址。如果一个端口 A 绑定了一个 MAC 地址，另一个端口 B 没有绑定 MAC 地址，端口 A 和 B 在同一个 VLAN，则拥有该 MAC 地址的用户不能通过交换机的端口 B 访问网络。如图 9-1 假设交换机的端口 1 绑定了 MAC 地址 00:10:5C:00:00:01，端口 2 没有绑定 MAC 地址，端口 1 和 2 属于同一个 VLAN，则用户 1 不能通过交换机的端口 2 访问网络，只能通过交换机的端口 1 访问网络。

当一个端口绑定了一个或多个 MAC 地址时，不会影响从这个端口输入的数据流的转发效率，数据流可以实现线速转发。一个端口最多可以绑定 128 个 MAC 地址。

端口绑定 MAC 地址与 802.1x 端口状态是互斥的。如果一个端口的 802.1x 状态已经设置为 Auto、Force-authorized 或 Force-unauthorized，那么这个端口不能绑定 MAC 地址。

10.2 MAC 绑定配置

iSpirit 2924G/2924F 交换机支持手工绑定 MAC 地址和自动绑定 MAC 地址。手工绑定 MAC 地址是用户通过命令逐个输入 MAC 地址与端口进行绑定。自动绑定 MAC 地址是把二层硬件转发表中该端口的已有的条目读出来直接进行 MAC 地址绑定。

如果一个端口已经绑定了MAC地址，此时自动绑定MAC地址无效，只能进行手工绑定MAC地址。自动绑定MAC地址只能在端口没有绑定MAC地址时进行。如果二层硬件转发表中该端口没有条目，自动绑定MAC地址无效，此时端口没有绑定任何MAC地址。如果二层硬件转发表中该端口的条目超过了128个，自动绑定MAC地址时只有前128个进行绑定。

iSpirit 2924G/2924F交换机缺省情况任何一个端口都没有绑定MAC地址。

●下面的命令在全局CONFIG模式下一个端口绑定MAC地址。如果不输入vlanid和mac-address参数，此时进行自动绑定MAC地址，把硬件转发表中相关的条目进行绑定MAC地址。如果输入vlanid和mac-address参数，进行手工绑定一个MAC地址，如果要手工绑定多个MAC地址，需要重复此命令：

mac bind <port> [<vlanid> <mac-address>]

注 意 ：

如果进行自动绑定MAC地址，MAC地址绑定无效或失败的原因可能如下：

该端口的802.1x状态已经设置为Auto、Force-authorized或Force-unauthorized。

该端口已经绑定了MAC地址。

二层硬件转发表中该端口没有条目。

如果进行手工绑定MAC地址，MAC地址绑定无效或失败的原因可能如下：

该端口的802.1x状态已经设置为auto、Force-authorized或Force-unauthorized。

该端口已经绑定了VLAN和MAC地址都相同的条目。

该端口已经绑定了128个MAC地址。

●下面的命令在全局CONFIG模式下解除一个端口的MAC地址绑定。如果不输入vlanid和mac-address参数，解除该端口下所有MAC地址绑定。若输入vlanid和mac-address参数，解除该端口下的一个指定MAC地址绑定：

no mac bind <port> [<vlanid> <mac-address>]

●下面的命令在全局CONFIG模式下显示MAC地址绑定信息。如果不输入port参数，显示所有的端口的MAC地址绑定信息。如果输入port参数，显示指定的端口的MAC地址绑定信息：

show mac bind [port]

10.3 MAC绑定配置实例

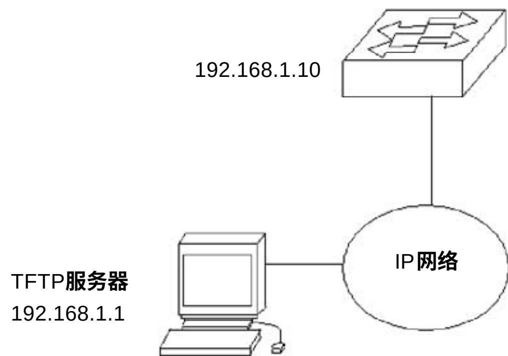


图10-2 MAC绑定实例

一个用户连接到iSpirit 2924G/2924F交换机的1端口，MAC地址为00:10:5c:af:ba:a9，为了安全起见，在这个端口上进行链路层的控制，只允许这个MAC地址的网卡的PC机能够通过1端口进行数据通信，在交换机上就要使用MAC绑定的功能

```
Switch# mac  bind  1  1  00:10:5c:af:ba:a9
Switch# show mac bind
port      vlan    macAddress       STATUS
1          1       00:10:5c:af:ba:a9     Active
```

如果不输入 vlanid **和** mac-address **参数，此时进行自动绑定** MAC **地址，把硬件转发表中相关的条目进行绑定** MAC **地址。**

如果进行自动绑定 MAC **地址，**MAC **地址绑定无效或失败的原因可能如下：**

1.**该端口的** 802.1x **状态已经设置为** Auto、Force-authorized **或** Force-unauthorized。

2.**该端口已经绑定了** MAC **地址。**

3.**二层硬件转发表中该端口没有条目。**

如果进行手工绑定 MAC **地址，**MAC **地址绑定无效或失败的原因可能如下：**

1.**该端口的** 802.1x **状态已经设置为** auto、Force-authorized **或** Force-unauthorized。

2.**该端口已经绑定了** VLAN **和** MAC **地址都相同的条目。**

3.**该端口已经绑定了** 128 **个** MAC **地址。**

第 11 章 配置堆叠

iSpirit2924G/2924F 交换机支持堆叠的功能，堆叠可以把多台物理上独立的交换机逻辑上看作是一台交换机。在实际的组网中，由于一台交换机的端口密度有限，满足不了用户的接入要求，需要把多台交换机堆叠在一起提供更多的端口和更高的交换容量。

本章对堆叠的技术和配置进行详细的描述，主要包括以下内容：

1、堆叠介绍

2、堆叠配置

3、堆叠配置示例

11.1 堆叠介绍

为了满足用户对接入交换机的越来越高的要求，联想网络公司推出了自有的堆叠技术，开发出了专用的堆叠模块，制定了专有的堆叠协议，可以对整个堆叠系统进行统一的管理。

本节对堆叠的技术进行详细的介绍，主要包括以下几个方面的内容：

1. 堆叠的好处

在接入交换机上使用堆叠技术可以给用户带来很多的实惠，主要表现在以下几个方面：

(1)使用支持堆叠技术的接入交换机可以扩展交换机的端口密度，一台交换机的端口密度是有限的，联想网络的堆叠技术可以把 32 台交换机堆叠在一起，一个堆叠系统中可以支持几百个甚至上千个端口，完全满足用户的接入要求。

(2)使用支持堆叠技术的接入交换机可以增加交换机的交换容量，传统的级连技术只能支持交换机之间的 1G 的带宽通道，但使用联想网络的专用的堆叠模块可以支持交换机间的更高的带宽通道，使堆叠系统中的数据流量更畅通。

(3)使用堆叠技术可以节省宝贵的 IP 地址资源，传统的组网中每台交换机至少需要一个 IP 地址，很浪费 IP 地址资源，而使用堆叠技术后，一个堆叠系统中的多台交换机只需要一个 IP 地址，可以大大节省 IP 地址资源 。

(4)使用堆叠技术可以简化网络的管理，传统的组网中每台交换机要进行单独管理，而使用堆叠技术后可以对整个堆叠系统进行统一管理，堆叠系统中的每台交换机当作一个模块。

总之，用户使用采用堆叠技术的交换机后，可以在组网时更加灵活，可以简化管理，可以降低成本，可以搭建方便易用的网络。

2. 堆叠的交换机类型

针对堆叠的概念，在网络中存在四种不同类型的交换机：命令交换机、成员交换机、侯选交换机和非堆叠交换机。管理员可以通过在交换机上配置使交换机成为不同类型的交换机。

命令交换机又被称为主交换机，在一个堆叠中只能存在一个命令交换机，命令交换机是整个堆叠的核心，给堆叠系统分配的 IP 地址必须配置在命令交换机上，通过命令交换机可以对整个堆叠系统进行管理。

成员交换机又被称为从交换机，它是一种临时的状态，交换机不能直接配置为成员交换机。当交换机被配置为侯选交换机并且打开自动加入堆叠的功能，当交换机发现了命令交换机后，该交换机就加入到堆叠中成为成员交换机。命令交换机可以发现这个堆叠中的所有成员交换机，并且可以对成员交换机进行管理。在一个堆叠中，最多可以有 32 个成员交换机。

当交换机配置为侯选交换机并且关闭自动加入堆叠功能，当交换机发现了命令交换机后，该交换机不会成为成员交换机，而是保持为侯选交换机。命令交换机可以发现这个堆叠中的所有侯选交换机，但不能对侯选交换机进行管理，但管理员可以在命令交换机上手工把侯选交换机变成成员交换机从而实现对该交换机的管理。

非堆叠交换机不会加入到任何堆叠中，它是一个单独的个体，必须直接对非堆叠交换机进行管理。

3. 堆叠的组网类型

在一个堆叠中，交换机可以有不同的拓扑方式进行连接，目前主要使用的组网方式有：菊花链方式、星型方式和组合方式。

如图 11-1 是菊花链堆叠的组网方式，在这个堆叠中有三台 iSpirit2924G/2924F 交换机以菊花链的方式相连，三台交换机用 25 和 26 堆叠口相连，其中的一台交换机的一个千兆端口连接到上层网络当作出口。三台交换机的 1 到 24 端口与接入网络相连，用户端的设备直接连在接入网络上。在这种组网方式中，可以指定任意一个 iSpirit2924G/2924F 交换机作为命令交换机。

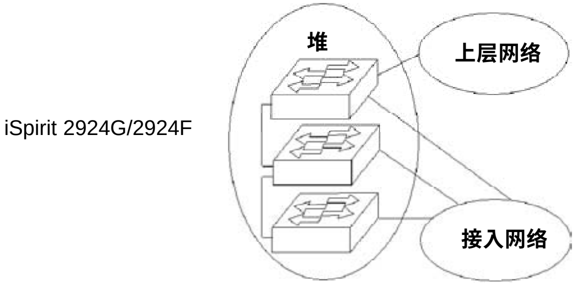


图 11-1 菊花链方式的堆叠

如图 11-2 是星型堆叠的组网方式，在这个堆叠中有一台 iSpirit2916G 交换机和三台 iSpirit2924G/2924F 交换机，每一台 iSpirit2924G/2924F 交换机的一个千兆端口与 iSpirit2916G 的一个千兆端口相连组成一个星型的堆叠。iSpirit2916G 的一个千兆端口与上层网络相连，三台交换机的 1 到 24 端口与接入网络相连，用户端的设备直接连在接入网络上。在这种组网方式中，最好指定 iSpirit2916G 交换机作为命令交换机。

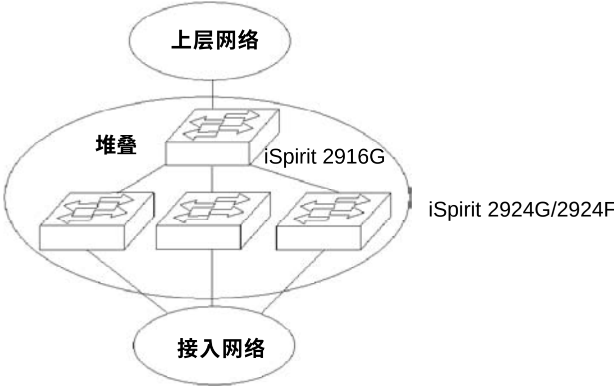


图 11-2 星型方式的堆叠

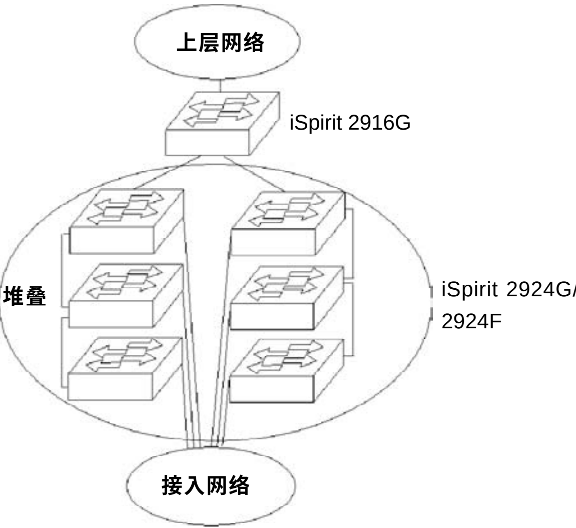


图 11-3 组合方式的堆叠

如图 11-3 是组合堆叠的组网方式，在这个堆叠中有一台 iSpirit2916G 交换机和六台 iSpirit2924G/2924F 交换机，有两组 iSpirit2924G/2924F 交换机以菊花链的方式相连，而这两组 iSpirit2924G/2924F 交换机与一台 iSpirit2916G 交换机以星型方式连接。iSpirit2916G 的一个千兆端口与上层网络相连，六台 iSpirit2924G/2924F 交换机的 1 到 24 端口与接入网络相连，用户端的设备直接连在接入网络上。在这种组网方式中，最好指定 iSpirit2916G 交换机作为命令交换机。

4.堆叠 VLAN

一个堆叠组必须在一个子网内，不能跨越子网，也就是说一个堆叠组必须在一个 VLAN 内，堆叠最好在 VLAN1 内建立。

在实际的组网中，需要把 VLAN1 当作管理 VLAN，所有堆叠的交换机相连的端口必须在 VLAN1 内，可以是 untagged 成员或者是 tagged 成员。如图 11-1 到 3，堆叠交换机之间相连的端口必须是 VLAN1 的成员，这样堆叠才能建立起来。接入网络的数据 VLAN 可以任意指定，可以不是 VLAN1。

5.堆叠端口

在一个堆叠组中，堆叠交换机之间相连的端口必须指定为堆叠端口。iSpirit2924G/2924F 交换机缺省 25 和 26 端口是堆叠端口，而其它端口不是堆叠端口。在用 25 和 26 端口做堆叠时，iSpirit2924G/2924F 交换机的 25 和 26 端口可以插入千兆模块，也可以插入堆叠模块，根据实际的应用而定。

如图 11-4 三台 iSpirit2924G/2924F 交换机组成一个菊花链式的堆叠，iSpirit2924G/2924F_1 交换机的 25 端口上连上层网络。在这样一个网络中，iSpirit2924G/2924F_1 交换机的端口 26 为堆叠端口，iSpirit2924G/2924F_2 交换机的端口 25 和 26 为堆叠端口，iSpirit2924G/2924F_3 交换机的端口 25 为堆叠端口。

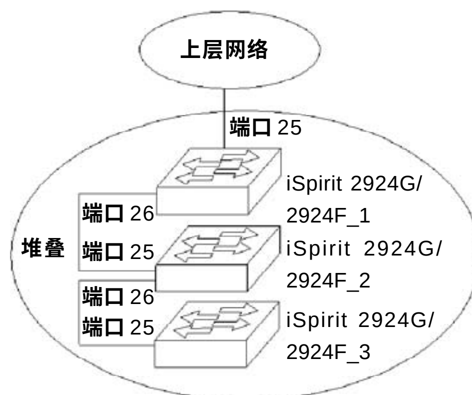


图 11-4 堆叠端口

6.堆叠管理

在一个堆叠组中命令交换机管理整个堆叠系统，命令交换机可以管理本交换机，也可以管理所有的成员交换机。命令交换机可以看到堆叠组中的侯选交换机的信息，但不能直接管理侯选交换机，必须手工把侯选交换机加入到堆叠组中成为成员交换机后才能对它进行管理。

对于 iSpirit2924G/2924F 交换机来说，目前可以在串口或 TELNET 终端上通过 CLI 的方式对堆叠组进行管理。不提供 WEB 管理方式对整个堆叠组进行管理，只能对单个交换机进行管理。堆叠组中的成员交换机可以被命令交换机管理，也可以在其上配置 IP 地址直接对其进行管理，如果要通过 SNMP 方式对成员交换机进行管理，必须在成员交换机上配置 IP 地址。

一个堆叠组中的命令交换机和成员交换机都会分配一个 UNIT 号，命令交换机的 UNIT 号总是 0，而成员交换机的 UNIT 号从 1 到 32，当交换机加入堆叠组成为成员交换机时，命令交换机会自动给该成员交换机分配一个 UNIT 号。当通过命令交换机管理成员交换机时，使用成员交换机的 UNIT 号来登录到成员交换机对其进行管理。

在一个堆叠组中，命令交换机识别成员交换机的唯一标识是成员交换机的 MAC 地址，但由于 MAC 地址不

好记忆，在每个交换机上都提供了一个堆叠系统名，为了方便记忆和简化堆叠的网络管理，管理员最好给堆叠组中的每个交换机都配置一个不同的堆叠系统名，这样便于定位堆叠中的成员交换机。

11.2 堆叠配置

堆叠的配置，主要包括以下内容：

1.堆叠缺省配置

iSpirit2924G/2924F 交换机堆叠缺省配置如下：

(1)交换机的类型缺省为侯选交换机，自动加入堆叠配置是打开的。

(2)交换机的 HELLO 间隔时间缺省是 60 秒。

(3)交换机的堆叠系统名缺省为 lenovo。

(4)交换机的堆叠端口缺省为 23 和 24 端口。

2.配置堆叠交换机的类型

堆叠交换机可配置的类型有三种，分别是：命令交换机、侯选交换机和非堆叠交换机。

下面的命令在全局配置模式下从非堆叠交换机变为侯选交换机，如果交换机已经是侯选交换机或命令交换机，此命令无效：

stack

下面的命令在全局配置模式下交换机从非堆叠交换机或侯选交换机成为命令交换机，如果该交换机已经是命令交换机或该堆叠组中已经有一个命令交换机，此命令无效：

stack commander

下面的命令在全局配置模式下交换机不再是命令交换机而成为侯选交换机：

no stack commander

下面的命令在全局配置模式下交换机从命令交换机或侯选交换机成为非堆叠交换机：

no stack

下面的命令在全局配置模式下打开自动加入堆叠配置，当交换机是侯选交换机并且发现了命令交换机时，该交换机自动加入堆叠并且成为成员交换机：

stack auto-join

下面的命令在全局配置模式下关闭自动加入堆叠配置，当交换机是侯选交换机并且发现了命令交换机时，该交换机不会成为成员交换机，继续保持为侯选交换机，当交换机是成员交换机但发现自动加入堆叠配置关闭时，该交换机会从成员交换机变为侯选交换机：

no stack auto-join

3.配置 HELLO 间隔时间

命令交换机每隔 HELLO 间隔时间会从所有的堆叠端口发 HELLO 包到网络中，当侯选交换机收到 HELLO 包可以发现命令交换机，根据自己的配置决定是否加入这个堆叠组而成为成员交换机。HELLO 间隔时间对于非命令交换机没有实际的用处。

下面的命令在全局配置模式下配置 HELLO 间隔时间：

stack hello-interval <interval>

4.配置堆叠系统名

下面的命令在全局配置模式下配置交换机的堆叠系统名，堆叠系统名可以用来标识一个堆叠组内的交换机，便于管理员对堆叠组进行管理：

stack host-name <name>

5.手工加入和退出堆叠

下面的命令在全局配置下把一个侯选交换机手工加入到堆叠中成为成员交换机，此命令只在命令交换机下配置有效，如果指定的 MAC 地址不是侯选交换机的 MAC 地址，则此命令无效：

stack member <mac-address>

下面的命令在全局配置模式下把指定的 UNIT 号的成员交换机手工退出此堆叠组成为侯选交换机，此命令只在命令交换机下配置有效：

no stack member <unit-number>

下面的命令在全局配置模式下把自己从堆叠组中退出成为侯选交换机，此命令只在成员交换机上有效，在命令交换机、侯选交换机和非堆叠交换机上此命令无效：

stack leave

6.登录到成员交换机

下面的命令在全局配置模式下登录到成员交换机，对成员交换机进行管理，此命令只在命令交换机下有效：

slave <unit-number>

7.显示堆叠信息

下面的命令在全局配置模式下显示堆叠的信息，如果是非堆叠交换机，此命令无效，如果是侯选交换机，只显示自身的基本信息，如果是成员交换机，显示自身和命令交换机的信息，如果是命令交换机，显示自身和所有的成员交换机的信息：

show stack

下面的命令在全局配置模式下显示所有的成员交换机的信息，此命令只在命令交换机上有效：

show stack members

下面的命令在全局配置模式下显示所有的侯选交换机的信息，此命令只在命令交换机上有效：

show stack candidates

下面的命令在全局配置模式下显示所有的成员交换机和侯选交换机的信息，此命令只在命令交换机上有效：

show stack all

下面的命令在全局配置模式下显示交换机的堆叠配置信息，包括堆叠的交换机类型、堆叠的 HELLO 间隔时间、堆叠系统名及堆叠端口等信息：

show stack configuration

11.3 堆叠配置示例

如图 11-4 所示，交换机 iSpirit2924G/2924F_1、iSpirit2924G/2924F_2 和 iSpirit2924G/2924F_3 组成菊花链式堆叠。假定选择 iSpirit2924G/2924F_1 作为命令交换机，端口 26 是堆叠端口，HELLO 间隔时间是 10 秒。iSpirit2924G/2924F_2 和 iSpirit2924G/2924F_3 交换机配置为侯选交换机并且自动加入堆叠配置为打开，iSpirit2924G/2924F_2 交换机的端口 25 和 26 是堆叠端口，iSpirit2924G/2924F_3 交换机的端口 25 是堆叠端口。

iSpirit2924G/2924F_1 **交换机的配置如下：**
Switch# stack hello-interval 10
Switch# stack host-name iSpirit2924G/2924F_1
Switch# stack commander

iSpirit2924G/2924F_2 **交换机的配置如下：**
Switch# stack host-name iSpirit2924G/2924F_2

iSpirit2924G/2924F_3 **交换机的配置如下：**
Switch# stack host-name iSpirit2924G/2924F_3

第 12 章 配置 QoS

本章描述如何通过 QoS 命令来配置 iSpirit 2924G/2924F 交换机的 QoS 服务。 针对 iSpirit2924G/2924F 交换机，对 QoS 的概念和实现作一个全面的介绍，为理解后面的内容做准备。 一步一步教您使用 QoS 命令对 iSpirit2924G/2924F 交换机进行 QoS 配置，这部分内容是本章的重点。

1、QoS 介绍

2、QoS 配置

当交换机没有配置 QoS 时，交换机使用同一个优先级转发所有通过交换机的数据流，不能保证数据流的可靠性、延时和吞吐量。

有些应用需要低延时，有些应用需要高可靠性，而有些应用则需要有稳定的吞吐量，这时就需要启动交换机的 QoS 功能，交换机可以对不同的数据流进行不同的优先级处理。

本章主要包括以下内容：

12.1 QoS 介绍

iSpirit2924G/2924F 交换机实现了强大的 QoS 功能。使用交换机的 QoS 功能，您能够让通过交换机转发的重要的数据流得到优先的处理，并对一些数据流进行带宽限制，使您的网络的带宽利用更加合理，网络性能变得可预 测 。

iSpirit2924G/2924F 交换机的每个端口最多有四个输出优先级队列，以 Q0，Q1，Q2，Q3 来标识各个输出队列，且 Q0 为最低优先级队列。可以配置 Q1，Q2，Q3 队列相对于 Q0 队列的输出包（Packet）比例，比例范围为 1~31。

输出调度为 WRR（Weighted Round Robin scheduling）模式时，输出调度引擎首先输出 Q3 队列的数据包，个数最多为 Q3 相对于 Q0 队列的输出包（Packet）比例大小，然后，依次如 Q3 输出 Q2，Q1，Q0 队列中的数据包。如此循环输出各个队列中的数据包，直到队列中的数据全部输出。

输出调度为 SPQ（Strict priority queue scheduling）模式时，只有当 Q3 队列的数据包输出完时，才能输出其他队列中的数据包。

可以根据如下几种策略划分业务的优先级：一、 802.1p 优先级标识。二、MAC 地址。三、端口。四、TOS/DSCP。对于一台交换机，TOS、DSCP 策略只能二选一。当这几种策略产生冲突时，按照如下策略优先级来解决冲突：1、端口优先级。2、MAC 地址优先级。3、802.1P 优先级。4、TOS/DSCP 优先级。当 TOS/DSCP 优先级和 802.1P 优先级优先级冲突时，谁能获得的输出优先级高，数据包就优先按照他输出。

不同的 QoS 使用不同的优先级标记，下面分别介绍三种 QoS 的标记：

●802.1p 的 QoS

802.1p 的 QoS 使用以太网帧中的 2 个字节的 TAG 标记中的最高三位作为其优先级，如图 12-1 所示。优先级的范围从 0 到 7。如果在 QoS 域中使用 802.1p 的 QoS，需要所有的数据包在网络上传输时都有 TAG 标记，比较适合在一个小范围的局域网中使用。

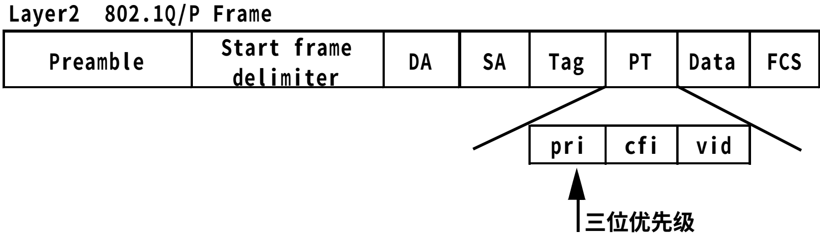


图 12-1 802.1p 的优先级位

●IP Precedence 的 QoS

IP Precedence 的 QoS 使用 IP 数据包头的 TOS 字段的最高三位作为其优先级，如图 12-2 所示。IP Precedence 的范围从 0 到 7。IP Precedence 的 QoS 在早期使用比较多，现在逐渐被 DiffServ 取代。

●DiffServ 的 QoS

DiffServ 的 QoS 使用 DSCP 作为其优先级标记，DSCP 位于 IP 数据包头的 TOS 字段的最高六位，如图 12-2 所示。DSCP 的范围从 0 到 63。

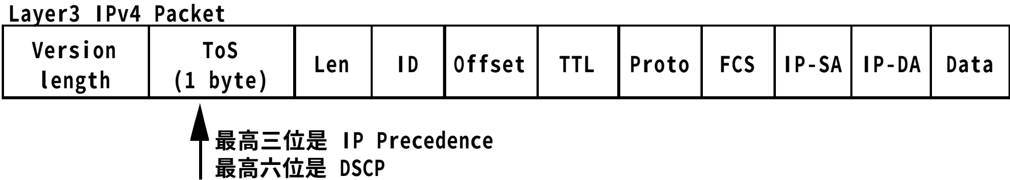


图 12-2 IP Precedence 和 DiffServ 的优先级位

常见术语

COS：802.1p 的业务类标记，值范围从 0 到 7，每个值标识一个业务类型。

IP Precedence：早期 IP 网络使用的一种业务类标记，值范围从 0 到 7，每个值标识一个业务类型。

DSCP：DiffServ 的业务类标记，值的范围从 0 到 63，每个值标识一个业务类型。

调度（scheduling）：根据调度策略对输出端口各个优先级队列中的 IP 数据包进行优先级处理，把 IP 数据包发送出去。

12.2 QoS 缺省配置

iSpirit2924G/2924F 交换机缺省情况下所有的端口都没有启用 QoS，所有的数据流以 best-effort 的方法转发。PORT、MAC、TOS/DSCP、COS 缺省优先级为 0。

QoS 的配置配置流程

1、根据选择的 QoS 配置策略，配置 COS、TOS/DSCP、PORT 和输出队列的映射表，或者配置 MAC 的优先级模式。

2、使能 QoS 的优先级配置。

各种 QoS 策略配置

1、COS 策略的配置

如下命令用于配置 COS 对于输出队列的映射表：

QoS COS-QUEUE <A，A-B COS VALUE> <OUT QUEUE>

如下命令用于禁止 COS 策略的配置：

NO QoS COS-QUEUE

如下命令用于显示 COS 策略的配置：

SHOW QoS COS-QUEUE [COS VALUE]

2、TOS/DSCP 策略的配置

如下命令用于配置 TOS 对于输出队列的映射表：

QoS TOS-QUEUE <A，A-B TOS VALUE> <OUT QUEUE>

如下命令用于配置 DSCP 对于输出队列的映射表：

QoS DSCP-QUEUE <A，A-B DSCP VALUE> <OUT QUEUE>

如下命令用于禁止 TOS/DSCP 策略的配置，对于一台交换机，TOS、DSCP 策略只能二选一：

NO QoS TOS-DSCP

如下命令用于显示 TOS/DSCP 策略的配置：

SHOW QoS DSCP-VALUE [DSCP VALUE]

SHOW QoS TOS-QUEUE [TOS VALUE]

SHOW QoS tosdscpstatus

3、PORT 策略的配置

如下命令用于配置 PORT 对于输出队列的映射表，PORT 策略的使能也包含此命令中：

QoS PORT-QUEUE <A,A-B PORT NUMBER><OUT QUEUE>

如下命令用于禁止 PORT 策略的配置：

NO QoS PORT-QUEUE <A，A-B PORT NUMBER>

如下命令用于显示 PORT 策略的配置：

SHOW QoS PORT-QUEUE <PORT NUMBER>

4、MAC 策略的配置

如下命令用于配置 MAC 优先级模式，对于包含此 MAC 地址的数据报文，根据配置模式，将此报文送到最高优先级输出队列。MAC 策略的使能也包含此命令中：

QoS MAC <PORT NUMBER> <VLANID><MAC ADDRESS><MODE>
MODE **说明：**
0 **：没有优先级配置。**1 **：依照源地址，设置优先级。**2 **：依照目的地址，设置优先级。**3 **：依照源和目的地址，设置优先级。**
如下命令用于禁止 PORT **策略的配置：**
NO QoS MAC <PORT NUMBER><VLANID><MAC ADDRESS>
如下命令用于显示 PORT **策略的配置：**
SHOW QoS MAC [PORT]

5**、输出调度策略的配置**
如下命令用于配置输出调度策略：
QoS SCHEDULE <MODE><WEIGHT1><WEIGHT2><WEIGHT3>
MODE **说明：**WRR： Weighted Round Robin
SPQ： Strict Priority Queueing
WEIGHT1、WEIGHT2、WEIGHT3**：为** Q1、Q2、Q3 **队列对于** Q0 **队列相的输出包（**Packet**）比例，也叫权重。**
如下命令用于显示输出调度策略：
SHOW QoS SHEDULE

第 13 章 配置管理服务

本章描述如何配置管理服务，主要包括以下的内容：

1、管理服务介绍

2、管理服务配置

13.1 管理服务介绍

在网络中，交换机本身的安全性至关重要，也是管理员非常关注的一个问题。iSpirit 2924G/2924F 交换机除了提供用户名和口令来控制交换机本身的安全以外，还提供了对管理服务的控制来实现交换机的安全。

iSpirit 2924G/2924F 交换机提供了 TELNET、WEB 和 SNMP 服务来实现交换机的远程管理，通过对这些服务的控制，如关闭或开启这些服务，把服务与 ACL 资源库联系起来等，来实现交换机管理的安全。

交换机管理除了串口外，还有 TELNET、WEB 和 SNMP 三种访问控制方式，后三种由于可以远程操作交换机，从而不受时间和地域限制，而备受管理员欢迎。但是随之而来的安全问题也不容忽视。特别是安全性要求高的地方，除了中心操作室的人员外，不允许外面的用户操作交换机，或者，只允许特殊的用户操作交换机，这时提供管理服务的控制的功能非常重要。

根据不同的需求，管理员可以关闭 TELNET、WEB 或（和）SNMP 服务，管理员或用户不能通过这些关闭的服务访问交换机。例如交换机关闭了 TELNET 服务，那一切试图通过 TELNET 登陆交换机的用户将不能成功。

当交换机的管理服务都被关闭时，设备可以获得很好的安全性。其实现方法主要是根据客户端和服务端通讯的原理，在服务对进入的用户管理信息进行判断，对于以上三种进入方式，判断管理员是否打开了相应的服务，如果没有打开，则用户不能使用该项服务登陆交换机。

如果管理员需要 TELNET、WEB 或（和）SNMP 服务，那需要的服务必须打开，此时拥有用户名和口令的用户可以从任何一台终端上从打开的这些服务管理交换机。这时交换机是非常不安全的，用户名和口令很容易被攻击者盗用，此时攻击者可以登陆到交换机上对设备进行破坏。

iSpirit 2924G/2924F 交换机通过管理服务与 ACL 相结合的方法实现打开的管理服务的安全性。交换机使用 ACL 资源库中的标准 IP 规则组对访问进行控制，只允许从合法的 IP 地址的终端访问交换机的服务，不允许非法的 IP 地址的终端访问交换机的服务。

当交换机的管理服务是打开的，通过使用 ACL 使设备获得很好的安全性。其实现方法主要是根据客户端和服务端通讯的原理，在服务对进入的用户管理信息进行判断，对于以上三种进入方式，判断管理员是否打开了相应的服务，如果服务是打开的，判断是否设置了 ACL，如果设置了 ACL，根据 ACL 的规则对源 IP 地址进行判断，如果源 IP 地址允许访问，则可使用该项服务管理交换机，如果源 IP 地址不允许访问，则不能使用该项服务管理交换机。

在交换机的管理服务使用 ACL 之前，需要配置好 ACL 资源库中的 ACL 规则，管理服务选用 ACL 资源库中的 ACL 规则，一个管理服务只能选用一个标准 IP 规则组。

如图 13-1 是一个管理服务控制的例子，假设用户 1 和用户 2 都知道交换机管理的用户名和口令。如果 TELNET 服务是打开的，那么用户 1 和用户 2 都可以通过 TELNET 服务管理交换机。如果 WEB 服务是关闭的，那么用户 1 和用户 2 都不可以通过 WEB 服务管理交换机。如果 SNMP 服务是打开的，但使用了 ACL 资源库中的一个标准 IP 规则组，该组规则只允许源地址为 192.168.0.100 通过，那么只有用户 1 可以通过 SNMP 服务管理交换机，用户 2 不能通过 SNMP 服务管理交换机。

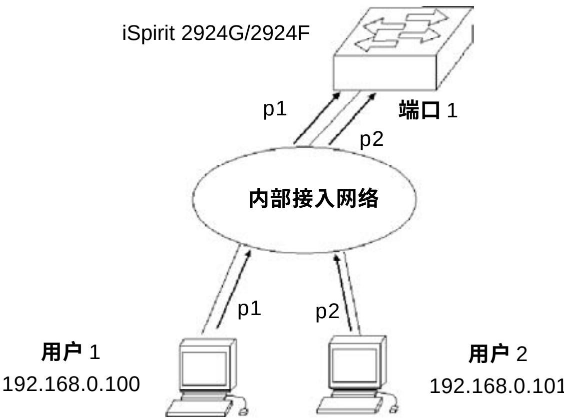


图 13-1 设备管理服务控制

13.2 管理服务配置

iSpirit 2924G/2924F 交换机缺省情况下 TELNET、WEB 和 SNMP 服务都是打开的。

●下面的命令在全局 CONFIG 模式下打开 TELNET 服务。如果不输入 group-id 参数，TELNET 服务打开但不使用 ACL 规则控制，用户可以从任何终端通过 TELNET 服务登陆交换机。如果输入 group-id 参数，TELNET 服务打开且使用 ACL 规则控制，只有 ACL 允许的 IP 地址的终端可以通过 TELNET 服务登陆交换机。group-id 的范围是从 1 到 199：

enable telnet [group-id]

●下面的命令在全局 CONFIG 模式下关闭 TELNET 服务，此时用户不能通过 TELNET 登陆交换机：

disable telnet

●下面的命令在全局 CONFIG 模式下配置 TELNET 的服务端口：

Switch# set telnet port <port-num>

●下面的命令在全局 CONFIG 模式下配置 TELNET 的登录密码：

Switch# set telnet password <password>

●下面的命令在全局 CONFIG 模式下打开 WEB 服务。如果不输入 group-id 参数，WEB 服务打开但不使用 ACL 规则控制，用户可以从任何终端通过 WEB 服务管理交换机。如果输入 group-id 参数，WEB 服务打开且使用 ACL 规则控制，只有 ACL 允许的 IP 地址的终端可以通过 WEB 服务管理交换机。group-id 的范围是从 1 到 199：

enable web [group-id]

●下面的命令在全局 CONFIG 模式下关闭 WEB 服务，此时用户不能通过 WEB 服务管理交换机：

disable web

●下面的命令配置在全局 CONFIG 模式 WEB 服务端口：

Switch# set web port [port-num]

●下面的命令在全局 CONFIG 模式下打开 SNMP 服务。如果不输入 group-id 参数，SNMP 服务打开但不使用 ACL 规则控制，用户可以从任何终端通过 SNMP 服务管理交换机。如果输入 group-id 参数，SNMP 服务打开且使用 ACL 规则控制，只有 ACL 允许的 IP 地址的终端可以通过 SNMP 服务管理交换机。group-id 的范围是从 1 到 199：

enable snmp [group-id]

●下面的命令在全局 CONFIG 模式下关闭 SNMP 服务，此时用户不能通过 SNMP 服务管理交换机：

disable snmp

●下面的命令在全局 CONFIG 模式下显示 TELNET、WEB 和 SNMP 服务的配置情况：

show manage-safety

13.3 SNMP 配置实例

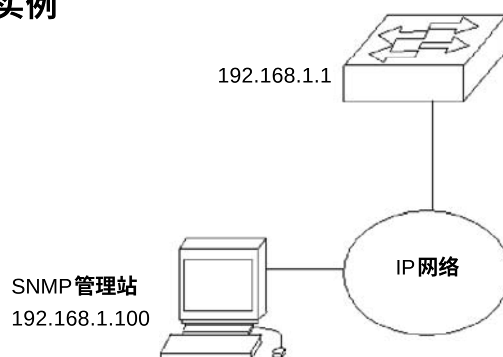


图 13-2 网络管理模型

有一个 SNMP 管理站上面运行 SNMP 管理软件，管理站的 IP 地址为 192.168.1.100，被管理的其中一台交换机的 IP 地址为 192.168.1.1。交换机和管理站之间并不需要在同一个 IP 网段，只需要之间 IP 能够相通就可以了。

在交换机上打开 SNMP，并且配置 snmp 的 community ，只读为 public

读写为 private

Switch# snmp community

Community Name : public
View Name(internet) :
ReadOnly(1),ReadWrite(2)
Permission : 1

Switch# snmp community
Community Name : private
View Name(internet) :
ReadOnly(1),ReadWrite(2)
Permission : 2

查看 snmp community **的配置**
Switch# show snmp community

CommunityName	ViewName	Permission	Status
public	internet	ReadOnly	Active
private	internet	ReadWrite	Active

这样配置一般就没有问题了
可选配置 trap
指的是当交换机发生特殊情况时，主动向 snmp **管理站发送** snmp **信息**
需要配置 trap **功能，选择** snmp **版本为** 2
Switch# snmp trap
trap name : test
Target Ip Addr: 192.168.1.100
snmpv1(1),snmpv2(2),snmpv3(3)
Version : 2
查看配置信息：
Switch# show snmp trap
————————————————————————————————-

Trap Name	: test
Transport Domain	: 1.3.6.1.6.1.1
Target ip	: 192.168.1.100
Target port	: 162
TimeOut	: 1500
Retry Count	: 0
Version	: snmp V2
Storage Type	: nonvolatile
Status	: Active

————————————————————————————————-
排 错 ：
如果 snmp **不起作用，需要查看以下几个方面**
1、**交换机上需要配置读写或只读的** community ,**例如只读为** pubic ,**读写为** private
2、**需要在** snmp **服务器上配置同样的** community，**才能够** snmp **服务器对交换机进行远程察看或者管理**

如果交换机不能主动发起 trap **信息给** snmp **服务器，需要查看以下：**
1、**交换机上需要配置读写或只读的** community ,**例如只读为** pubic ,**读写为** private
2、**需要在交换机上设置** trap **接收者的** ip **地址，也就是** snmp **服务器的** ip **地址**
3、**确保交换机的** ip **地址和** snmp **服务器之间的** ip **是能够相通的**

第 14 章 配置 SNMP 和 RMON

iSpirit 2924G/2924F 交换机提供了 SNMP 和 RMON 对交换机进行远程管理。本章描述如何配置 SNMP 和 RMON，主要包括以下内容：

1、SNMP 介绍
2、RMON 介绍
3、SNMP 配置
4、RMON 配置

14.1 SNMP 介绍

SNMP 是简单网络管理协议，是目前使用最广泛的网络管理协议，它具有五大功能：故障管理，计费管理，配置管理，性能管理，安全管理。它提供网管应用软件和网管代理（agent）之间通信的信息格式。

SNMP 网络管理协议有四大要素：管理工作站，管理代理，管理信息库，网络管理协议。管理代理在交换机上，是管理工作站访问交换机的服务端，管理工作站访问网管代理的信息以 MIB 的形式组织，形成管理信息库。

SNMP 有三大操作：GET 操作，SET 操作，TRAP 操作。GET 操作使管理工作站能够获取代理中对象的值。SET 操作使管理工作站能够设置代理中对象的值。TRAP 操作使代理能够想管理工作站通告重要事件。

TRAP 消息是当交换机发生事件时主动发给管理工作站的，这些消息包括冷启动，热启动，端口的 link up、link down，共用体名的认证失败，STP 的状态切换，RMON 的 EVENT 被触发的信息等。

目前 SNMP 有三个版本：SNMPV1，SNMPV2，SNMPV3 个，后面的版本是前面的升级版，功能进行了增强，安全性得到提高。iSpirit 2924G/2924F 交换机支持所有的三个 SNMP 版本，可以对三个版本的 SNMP 协议包进行解析。当发送 TRAP 消息时，可以使用 SNMPV1，SNMPV2 和 SNMPV3 中的任何一个版本发送。

iSpirit 2924G/2924F 交换机支持 MIB1 和 MIB2 两种 MIB 类型对象，同时支持大量的 RFC，BRIDGE 和私有的 MIB 对象，通过 SNMP 可以完全管理交换机。下面列出了 iSpirit 2924G/2924F 交换机支持的一些 MIB：

RFC 1213 **RFC1213-MIB** MIB II All groups except egp and transmission.

RFC 1493 **BRIDGE-MIB dot1dBase** and **dot1dStp** groups.

RFC 1757 **RMON-MIB** RMON-Lite (4 RMON1 groups)1-statistics, 2-history, 3-alarm, and 9-event.

RFC 1907 **SNMPv2-MIB** Conformance groups 5, 6, 7, 8, 9.Also used for SNMPv3.

RFC 2233 **IF-MIB** Interface group extension for SMIv2CG= 4, 5, 6, 7, 10, 11, 13.

RFC 2571 **SNMP-FRAMEWORK-MIB** SNMPv3 MIB. SNMP ManagementFrameworks. CG=1.

RFC 2572 **SNMP-MPD-MIB** SNMPv3 MIB. SNMP Message Processing and Dispatching. CG=1.

RFC 2573 **SNMP-TARGET-MIB** SNMPv3 MIB. Define management targets. CG=1, 2, 3.

SNMP-NOTIFICATION-MIB SNMPv3 MIB. Notification generation configuration. CG=1, 2.

RFC 2574 **SNMP-USER-BASED-SM-MIB** SNMPv3 MIB. Define SNMP USM.CG=1.

RFC 2575 **SNMP-VIEW-BASED-ACM-MIB** SNMPv3 MIB. Define SNMP VACM.CG=1.

RFC 2665 **EtherLike-MIB dot3StatsTable** group for SMIv2.

如图 14-1 是管理工作站与管理代理之间的 SNMP 协议交互的例子。管理工作站可以通过发送 Get Request、Get_next Request 和 Set Request 的 SNMP 消息访问交换机管理代理，获取或设置交换机的 MIB 对象的值，交换机管理代理回送 Get Response 的 SNMP 消息给管理工作站。当交换机上发生了一些事件时，交换机的管理代理主动发送 SNMP TRAP 消息给管理工作站。

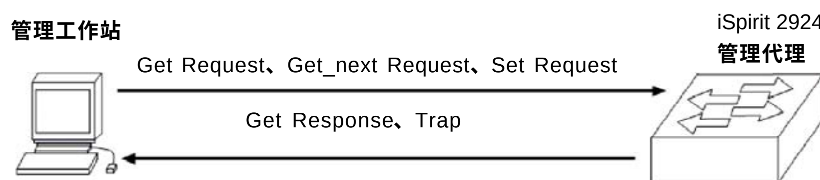


图 14-1 管理工作站和管理代理之间的 SNMP 协议交互

14.2 RMON 介绍

RMON(Remote Network Monitoring, 远程网络监测)作用于定义标准的网络监视功能和接口，使基于 SNMP 的管理终端和远程监视器之间能够通信。RMON 提供了两种控制特征：配置和操作调用。

1.配置

远程监测器需要为数据采集进行配置。配置指定要采集的数据类型和形式。RMON MIB 被分成一定数量的功能组，在每一组内部，有一个或多个控制表和一个或多个资料表。控制表是典型可以读写的表，包含资料表中的资料参数，而资料表是只读的。这样，在配置时，管理终端设定合适的配置参数来配置远程监视器来采集想要的数据。

2.操作调用

操作调用是 SNMP 通过 set 操作来发送一个命令。

RMON 表管理的操作包括：添加、删除，修改和读取。RMON 在进行表操作时都要涉及到行字段操作。在 statistics 组中的 etherStatsStatus，history 组中的 historyControlStatus，alarm 组中的 alarmStatus 和 event 组中的 eventStatus。他们的取值都是 valid(1), createRequest(2),UnderCreation(3)和 invalid(4)。

添加：在添加行时先对行字段作 createRequest（2）操作，完成操作后行字段状态自动迁移到 underCreation（3）；当配置完其它的有效字段操作后，再对行字段作 valid（1）操作，行字段变为 valid（1）。

修改：当要修改表项时，需要先配置行字段为 underCreation（3），再修改其它字段，修改完后,对行字段作 valid（1）操作，行字段变为 valid（1）。在行字段为 valid（1）状态下，不能修改其它字段。

删除：配置行字段状态为 invalid（4）就可以删除一行。

iSpirit 2924G/2924F 交换机支持 1、2、3、9 组 RMON MIB，分别是 statistics 组，history 组，alarm 组和 event 组。

14.3 SNMP 配置

SNMP 配置包括交换机的 community 配置和 TRAP 工作站的配置。iSpirit 2924G/2924F 交换机缺省有一个只读的共用体，共用体名为 public，交换机最多可以配置 8 个共用体。iSpirit 2924G/2924F 交换机缺省没有配置 TRAP 工作站，交换机最多可以配置 8 个 TRAP 工作站。

SNMP 的命令如下：

- snmp community

  模式：CONFIGURATION

  参数：参数以交互式输入

  Community Name：共用体名称

  Permission：读写权限，1)只读，2)读写

  功能：配置访问网管的共用体名称，这是一个交互式命令。配置时用户可以根据提示输入需要的创建的共用体名称，和读 / 写权限。

- snmp trap

  模式：CONFIGURATION

  参数：参数以交互式输入

  trap name：trap 名称

  Target Ip Addr：Trap 发送的目标 IP 地址

  Version：Trap 发送的版本 v1，v2，v3

  功能：添加或修改 snmp trap 的发送目标。这是一个交互式命令。Trap name 是唯一的，如果修改了已经存在的 name，则可以修改这个 trap 发送目标项。Target ip addr 是发送 trap 的目标地址；version 是以 snmpV1，snmpV2 还是 snmpV3 的方式发送。这个命令缺省配置了目标端口是 162。

- show snmp trap

  模式：CONFIGURATION

  功能：显示所有的 trap 配置。

- no snmp trap <trap-name>

  模式：CONFIGURATION

  功能：删除指定 name 的 trap 项。

- snmp trap ip <trap-name> <ip-address>

  模式：CONFIGURATION

  参 数 ：

  trap-name：Trap 名称

  ip-address：目标 IP 地址

功能：修改指定 trap-name 的目的 ip 地址为 ip-address

- snmp trap port <trap-name> <port>

模式：CONFIGURATION
参 数 ：
trap-name：Trap 名称
port：目标端口
功能：修改指定 trap-name 的目的 port。

- snmp trap retries <trap-name> <retries>

模式：CONFIGURATION
参 数 ：
trap-name：trap 名称
retries：重发次数
功能：修改指定 trap-name 的 trap 项的重发次数为 retries 次。SnmpV1 不支持这个参数。

- snmp trap timeout<trap-name> <timeout>

模式：CONFIGURATION
参 数 ：
trap-name：Trap 名称
retries：超时时间
功能：修改指定 trap-name 的 trap 项的发送超时为 timeout，timeout 的单位是 1/100 秒，SnmpV1 不支持这个参数。由于 udp 没有确认机制，所以配置了 retries 和 timeout 时，每条 trap 会间隔 timeout/100 秒发送 retries 次。

- snmp trap version <trap-name><version>

模式：CONFIGURATION
参 数 ：
Trap-name：Trap 名称
version：发送版本
功能：修改指定 trap-name 的 trap 项的发送版本。

14.4 RMON 配置

RMON 的命令如下：

- rmon alarm [index]

模式：CONFIGURATION
参 数 ：
index：索引，Index 是可选项，如果没有输入系统缺省生成一个 index 值。
rmon alarm 命令是一个交互式命令，如果输入了 index 则添加或修改指定的组。下面介绍 alarm 交互式输入字段：
Interval：间隔取值时间，单位为秒。（建议取值 2 秒）
Variable：被监视的节点。类型必须是 INTEGER (INTEGER, Counter, Gauge,or TimeTicks)
SampleType：计算要与阀值比较的数值的方法。如果该对象的取值为 absoluteValue (1)，则所选变量的取值直接和阀值相比较。如果该对象的取值为 deltaValue(2)，则在所选变量的上一个采用的取值减去当前值后，起差值于阀值相比较。
StartupAlarm：取值为 risingAlarm(1), fallingAlarm(2), risingOrFallingAlarm(3)。指定在一行有效后，risingThreshold 时第一个取样大于或等于，fallingThreshold 时小于或等于，或者两者都是时是否产生警告。
RisingThreshold：取样统计的上限阀值。
RisingEventIndex：当超过上限时所用的 eventEntry 索引。
FallingThreshold：取样统计的下限阀值。
FallingEventIndex：当超过下限时所用的 eventEntry 索引。
功能：alarm 组用来定义网络性能的一系列阀值。如果阀值在某一方面被超过以后，就会产生警告。Alarm

组由一个表 alarmtable 组成。表中的每一条目都规定了要监视的特定变量，取样时间间隔和阀值参数。

- rmon event [index]

  模式：CONFIGURATION

  参 数 ：

  index：索引，Index 是可选项，如果没有输入系统缺省生成一个 index 值。

  功能：event 组支持事件定义。事件由 MIB 其它地方的条件所引发，时间也能引发定义在 MIB 其它地方的动作。事件可能导致该组中记录信息，或是发出 SNMP Trap 消息。

  rmon event 命令是一个交互式命令，如果输入了 index 则添加或修改指定的组。下面介绍 event 交互式输入字段中 EventType：事件类型，none(1)，log(2)，snmp-trap(3)，log-and-trap(4)。

- no rmon alarm <index>

  模式：CONFIGURATION

  参 数 ：

  index：索引。

  功能：删除指定索引 index 的 alarm 配置 entry 项。

- no rmon event <index>

  模式：CONFIGURATION

  参 数 ：

  index：索引。

  功能：删除指定索引 index 的 event 配置 entry 项。

- show rmon configuration alarm [index]

  模式：CONFIGURATION

  参 数 ：

  index：索引。

  功能：显示 alarm 的配置表，如果输入了 index 则显示指定 index 的配置项，否则显示全部配置项。

- show rmon configuration even [index]

  模式：CONFIGURATION

  参 数 ：

  index：索引。

  功能：显示 event 的配置表，如果输入了 index 则显示指定 index 的配置项，否则显示全部配置项。

- show rmon table even [index]

  模式：CONFIGURATION

  参 数 ：

  index：索引。

  功能：显示 event 的资料表，如果输入了 index 则显示指定 index 的配置项，否则显示全部配置项。

- show rmon table statistics [index]

  模式：CONFIGURATION

  参 数 ：

  index：索引。

  功能：显示 statistics 的资料表，如果输入了 index 则显示指定 index 的配置项，否则显示全部配置项。

第 15 章 配置调试工具

本章对这些调试工具的使用和配置进行详细的描述，主要包括以下内容：

１、**调试工具介绍**

２、**调试工具配置**

15.1 调试工具介绍

在实际应用中，网络经常会出现一些故障或问题，需要有一些工具来对问题进行跟踪和定位。ISpirit 2924G/2924F 交换机提供了多种调试工具，可对交换机本身或网络中的一些问题进行跟踪和定位。

iSpirit 2924G/2924F 交换机提供了多种调试工具，主要有：PING 工具、TELNET 客户端工具。

本节对这些调试工具进行详细的描述，主要包括以下内容：

●TELNET 客户端工具介绍

1. TELNET客户端工具介绍

iSpirit 2924G/2924F 交换机提供一个 TELNET 客户端工具，可以从交换机上 TELNET 到另一个设备上，对设备进行配置和管理。

iSpirit 2924G/2924F 交换机有一个串口终端和 5 个 TELNET 终端，从串口终端或 TELNET 终端上可以执行 TELNET 命令登陆到目的设备，对目的设备进行管理。ISpirit 2924G/2924F 交换机只支持一个 TELNET 客户端，当 TELNET 客户端已被一个终端使用时，另外的终端不能使用 TELNET 客户端，必须等到使用 TELNET 客户端的终端退出时才能使用 TELNET 客户端。

15.2 调试工具配置

本节介绍 TELNET 客户端工具配置：

1. TELNET客户端工具配置

iSpirit 2924G/2924F 交换机提供了一个 TELNET 命令，从 1 个串口终端或 5 个 TELNET 终端上可以执行 TELNET 命令登陆到目的设备，但 TELNET 客户端同时只能被一个终端使用。

下面的命令在全局 CONFIG 模式下登陆到目的设备：

telnet <ip-address>

第 16 章 WEB 页面的设置

本章主要以 iSpirit 2924G **举例说明以下内容：**

1、WEB **页面综述**

2、**各页面详细介绍**

16.1 WEB 页面综述

1.WEB 访问的特点

联想天工 iSpirit2924G/2924F 交换机为用户提供 Web 访问功能。用户可以通过 Web 浏览器访问交换机，对交换机进行管理和配置。WEB 访问的主要特点是：

- 易于访问：用户可以从网络的任何地方轻松访问交换机。
- 用户可以用熟悉的 Nestscape Communicator 和 Microsoft Internet Explorer 等浏览器对联想天工 iSpirit2924G/2924F 交换机的 WEB 页面进行访问，WEB 页面以图形化和表格化的形式呈现给用户。
- iSpirit2924G/2924F 交换机提供了丰富的 WEB 页面，用户可以通过这些 WEB 页面对交换机的绝大部分功能进行配置和管理。
- 支持中英文 WEB 页面，用户可以根据需要选择中文或英文 WEB 页面对交换机进行管理。WEB 页面功能的分类整合，便于用户找到相关的页面进行配置和管理。

2.WEB 浏览的系统需求

Web 浏览的系统需求如表 16-1 所示。

表 16-1：

硬件与软件	系统需求
CPU	奔腾586以上
内存	32MB以上
分辨率	800x600以上
颜色	256色以上
浏览器	IE4.0以上或Netscape4.01以上
操作系统	Microsoft? ,Windows95? ,Windows98? ,WindowsNT? , Windows2000? ,WindowsXP? ,WindowsME? ,Linux,Unix类操作系统

注 意 ：

Microsoft®，Windows95®，Windows98®，WindowsNT®，Windows2000®，WindowsXP®，Windows ME® 是微软公司的注册商标，所有其它产品名，商标，注册商标和服务标记，版权由各自所有者持有。

3.WEB 浏览会话的登陆

在启动 Web 浏览会话前用户需要确认：

- 已经对交换机进行了 IP 配置，交换机的 VLAN1 的接口 IP 地址是 192.168.0.1，子网掩码是 255.255.255.0。
- 已将一台安装有 Web 浏览器的主机连接到网络上，并且主机能够 PING 通交换机。

完成以上两项工作后，用户在浏览器的地址栏输入交换机的地址并按回车后即可进入交换机 Web 登录页面，如图 16-1 所示。iSpirit2924G/2924F 交换机缺省用户名是 admin，缺省密码为空。



图 16-1 登陆界面

4.WEB 页面基本组成

以 2924G 为例说明，操作如图 16-2，WEB 页面主要由三部分组成：标题页、导航树页和主页面。

标题页　　　用于显示徽标。

导航树页　　WEB 页面的结点，用户可以打开树上的文件夹，从中选择要打开的页面。

主页面　　　用于显示用户从导航树中选择的页面。



图 16-2 Web 页面结构

5.导航树结构

图 16-3 显示导航树的组织结构。导航树位于每一页面的左下方，用树的方式显示 WEB 页面的结点，用户可以很方便地找到要管理的 WEB 页面。根据网页功能的不同将其划分成不同的组，每组中包括一个或多个页面。大多数导航树中的网页名是相应的网页上部的网页标题的缩写。



图 16-3 导航树结构

6.页面按钮介绍

在页面上有些通用的按钮，这些按钮的作用一般是一样的，表 16-2 对这些按钮的作用进行介绍。

表 16-2：

按钮	作用
Refresh	更新页面上的所有域
Apply	将更新过的数值放到内存中。因为错误检查由Web服务器完成，所以在用户选择该按钮前，没有错误检查
Save	做Apply的动作，并且在非易失存储器中存储所有配置变量。因为存储操作需要擦写Flash芯片，这要占用一定时间，所以建议用户在做完所有改动之后，再按Save按钮。
Delete	删除当前记录。

7.出错信息

如果交换机的 WEB 服务器在处理用户请求时出现错误，就会在一个对话框中显示相应的出错信息。图 16-4 显示一个出错信息对话框。



图 16-4 出错信息

8.条目域

有一些页面在表的最左列有一个条目域(Entry)，如图 16-5 所示，通过该域可以访问表中的不同行。当你选择条目域的某个值时，那一行的相应信息就显示在首行，这时只有该行可被编辑，该行又称为活动行。当最初加载一页时，条目域显示 new，活动行为空。

如果想加入新行，要从条目域的下拉菜单中选择 new，输入新行信息，然后按存储（SAVE） 或应用（Apply）键。

如果想编辑已经存在的行，要从条目域的下拉菜单中选择相应的行号，根据需要编辑改行，然后按存储（SAVE）或应用（Apply）键，你会看到相应的改变在该表中显示出来。

如果想删除一行，要从条目域的下拉菜单中选择相应的行号，然后按删除（Delete）键，该行会从该表中消失。



图 16-5 条目域

9.状态域

有一些页面在表的最右列有一个状态域（Status），如图 16-6 所示，该域显示该行状态。由于所有行状态的改变都是在内部处理完成，所以该状态域是只读的。一旦一行中所有域信息都生效，该行状态就自动变成活动态 active。

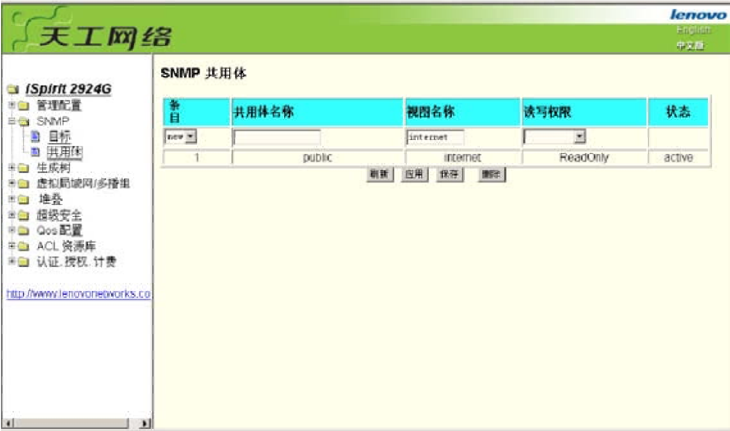


图 16-6 状态域

16.2 WEB 页面介绍

iSpirit2924G 交换机的 WEB 页面组织成组，每组包括一个或多个 WEB 页面。下面逐个对各个页面进行介绍。

1.登录对话框

图 16-7 显示登录对话框，该登录对话框在用户第一次登录网页时显示。用户在相应的字段输入用户名及密码，然后按下 OK 键就可以登录到交换机的 Web 服务器。密码区分大小写，并且最多可以设置 16 个字符。iSpirit2924G/2924F 交换机缺省用户名是 admin，缺省密码为空。



图 16-7 登录对话框

2.主页面

图 16-8 显示联想天工 iSpirit2924G 交换机的 WEB 主页面。该页面会在用户登录网页后或点击导航树中的 iSpirit2924G 结点后显示出来。



图 16-8 主页面

3.管理配置

（1）交换机配置页面

图16-9是交换机配置页面，用户可以通过该页对交换机的基本信息进行配置。

用户可以配置交换机的默认网关（缺省路由）。用户可以看到交换机的VLAN1子网的MAC地址，但不能进行配置。

用户可以启动或关闭一些基本的协议，如STP、IGMP SNOOPING协议。

用户可以通过此页面重启交换机，用户从Reset下拉菜单中选择reset或者reset factory defaults，然后按下应用（Apply）或保存（Save）键。在交换机重启前，将提示用户确认选择。如果用户选择reset，只是重启交换机，如果用户选择reset factory defaults，重启交换机并让交换机回到出厂缺省配置状态。

图16-9 管理配置页面

（2）系统配置页面

图16-10是系统配置页面，该页提供一些交换机的系统信息给用户，并允许用户对其中的一些系统信息进行配置。

用户可以通过该页面查看交换机的系统描述、系统的OID、系统的端口个数和系统的启动时间。用户可以配置交换机的系统名字、系统位置、系统联系和产品名称。

图16-10 系统配置页面

（3）端口配置 / 统计信息页面

图 16-11 是端口配置 / 统计信息页面。用户可以通过该页面启用或禁用端口，设置端口速度，或查看端口的基本信息及统计信息。

为设置或查看某一特定端口，用户需要从 Module 和 Port 的下拉菜单中选择相应的数字。端口状态缺省为 enable，可以选择下拉菜单中的 disable 来禁用端口。用户也可以选择设置速率下拉菜单对端口的速率进行设置，如对端口进行强制半双工 10M 等。用户可以通过此页面查看端口的其它基本信息和收发包的统计信息。



图 16-11 端口配置 / 统计信息页面

（4）串口配置页面

图 16-12 是串口配置页面，该页显示串口波特率及其它与串口相关的信息。当主机通过串口终端（如 Windows 的超级终端）对交换机进行管理时，串口终端上的 COM 口配置必须与本页面的信息一致。



图 16-12 串口配置页面

（5）密码修改页面

图 16-13 是密码修改页面，通过此页面用户可以修改交换机的管理密码，串口、TELNET 和 WEB 管理使用同一个密码。密码区分大小写，并且最多可以设置 16 个字符。

如果要修改密码，用户需要输入两次新密码，一旦用户按下应用（APPLY）或存储（SAVE）键，新密码就被激活，这时会显示登录对话框（如图 16-7 所示），需要用户重新登录网页，用户必须输入新密码登录 WEB 页面。



图 16-13 密码修改页面

（6）端口聚合配置页面

图 16-14 是端口聚合配置页面。该页面允许用户配置端口聚合。该页面由三部分构成：端口聚合组号选择、端口列表选择和端口聚合方法选择。

为创建或修改端口聚合，用户需要选择一个端口聚合组号，端口聚合组号从 0 到 3。用户点击列表框中相应的端口聚合组号，该端口聚合的信息显示在活动行中，用户可以在活动行中选择端口聚合的方式和聚合的端口列表。当设置好后，按下应用（Apply）或存储（SAVE） 键。

交换机提供了 4 种端口聚合方式：基于源 MAC 地址，基于目的 MAC 地址，基于源与(AND)目的 MAC 地址，基于源异或(XOR)目的 MAC 地址。其中数据包的二层转发可以使用所有的 4 种端口聚合方式.

iSpirit2924G 交换机最大支持 4 组端口聚合，每组端口聚合最多支持 8 个端口。



图 16-14 端口聚合配置页面

（7）端口带宽配置

图 16-15 是端口带宽配置页面，可以对端口限速进行配置，限速方式可配置为单向接收限速，单向发送限速，双向限速。限速粒度为 64 kbytes.



图 16-15　端口带宽配置页面

（8）端口镜像配置页面

图 16-16 是端口镜像配置页面，该页面允许用户配置端口镜像。端口镜像是通过镜像端口监听被镜像输出端口输出的数据包和被镜像输入端口输入的数据包。iSpirit2924G 交换机只能有一对镜像端口和被镜像端口。



图 16-16　端口镜像配置页面

4.SNMP 配置

（1）SNMP　TRAP 配置页面

图 16-17 是 SNMP TRAP 配置页面，该页面允许用户配置接收 TRAP 消息的工作站的 IP 地址以及 TRAP 协议包的一些参数，总共可以配置 8 个条目。

缺省情况下该页面的表中存在三个条目，它们处于非活动状态，表示不可以使用，可以删除其中两个，但不允许全部删除，即表中至少有一项要保留。

在配置条目时，缺省参数是 TRAP 的目的端口号是 162，TRAP 包不重发，如果重发超时时间间隔为 15 秒以及 SNMP 版本为 SNMPV1 版本。这些参数用户都可以修改，如果设置成功，条目中的状态会显示成为 active。如果配置成功，SNMP　TRAP 功能将会起作用，一旦发生 link　up 或 link　down 等情况，交换机将会自动向目标地址发送 TRAP 包。



图 16-17 SNMP TRAP 配置页面

（2）SNMP 共用体配置页面

图 16-18 是 SNMP 共用体配置页面，该页面允许用户配置交换机的共用体的名称和读写权限，总共可以配置 8 个条目。

缺省情况下交换机有一个 public 名的共用体，该共用体是只读权限。与此对应，该页面上只有一个活动的条目，共用体名是 public，权限是只读权限。当交换机需要通过 SNMP 进行网管时，需要配置一个可读可写权限的共用体。视图名称参数缺省是 internet，用户在配置共用体时最好不要修改此参数。



图 16-18 SNMP 共用体配置页面

5.生成树（STP）配置

（1）生成树桥(Bridge)参数配置页面

图 16-19 是生成树桥(Bridge)参数配置页面，该页面允许用户查看生成树指定根的信息及生成树桥的配置信息，同时用户还可以修改生成树桥的配置信息。

用户可以修改生成树桥的优先级，优先级的缺省值是 32768。桥的优先级越小，桥成为根的可能性越大。建议用户在一般情况下不要修改该页面上的时间参数，因为这些参数的值是 STP 协议的缺省标准值。

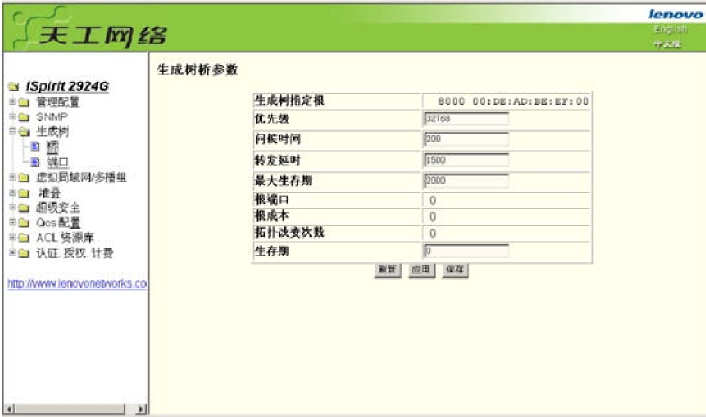


图 16-19 生成树桥(Bridge)参数配置页面

（2）生成树端口参数配置页面

图 16-20 是生成树端口参数配置页面，该页面允许用户查看所有端口的生成树端口参数，并能对端口的 STP 状态和优先级进行配置。

用户可以通过设置端口的 STP 状态为 disable 来禁止该端口参加 STP 计算。用户可以修改端口的优先级，端口的优先级缺省为 128，端口的优先级越小，端口成为根端口的可能性就越大。



图 16-20 生成树端口参数配置页面

6.虚拟局域网 / 多播组配置配置

（1）当前 VLAN 配置页面

图 16-21 显示当前 VLAN 配置页面。该页面是只读页，显示当前的所有的 VLAN 配置信息，包含 VID 和端口列表。

一个端口可以不是 VLAN 的成员，可以是 VLAN 的 tagged 成员或 untagged 成员。在页面的端口上的字符含义如下表 16-3 所示：

表 16-3：

字符	全称	含义
-	Non-member	该端口不是这个VLAN的成员
M	Member	该端口是这个VLAN的tagged成员
U	Untagged	该端口是这个VLAN的untagged成员



图 16-21 当前 VLAN 配置页面

（2）静态 VLAN 配置页面

图 16-22 是静态 VLAN 配置页面，该页面允许用户创建一个 VLAN 和配置一个 VLAN 的端口成员。该页面由两部分构成：活动行和列表框。活动行在首行，可编辑，活动行下方的列表框包含一系列的以 VID 和 VLAN 名的静态 VLAN。

如果要创建一个新的 VLAN，用户在活动行输入 VID、VLAN 名及端口列表信息，然后按下应用（Apply）或存储（SAVE）键，这时列表框会显示用户创建的 VLAN 的 VID 和 VLAN 名。

如果要修改一个已经存在的 VLAN，用户需要点击列表框中相应的 VLAN。该 VLAN 将显示在活动行中，用户可以修改该 VLAN 的 VLAN 名和端口列表信息。当修改结束后，按下应用（APPLY）或存储（Save）键。

如果要删除一个 VLAN，用户需要点击列表框中相应的 VLAN。该 VLAN 将显示在活动行中，按下删除（Delete）键可以删除该 VLAN，同时该 VLAN 的信息将从列表框中去除。

iSpirit2924G 交换机最多支持 255 个 VLAN，VLAN ID 的范围是 1 到 4094。一个端口可以不是 VLAN 的成员，也可以是 VLAN 的 tagged 成员或 untagged 成员。当修改 VLAN 的端口列表时，在每一个端口处点击鼠标，可以在株 - 、U、M 之间进行切换。在页面的端口上的字符含义如下表 16-4 所示：

表 16-4：

字符	全称	含义
-	Non-member	该端口不是这个VLAN的成员
M	Member	该端口是这个VLAN的tagged成员
U	Untagged	该端口是这个VLAN的untagged成员



图 16-22 静态 VLAN 配置页面

（3）当前多播组配置页面

图16-23是当前多播配置页面，该页面是只读页，显示当前存在的所有多播组，包括IGMP SNOOPING学习到的和静态配置的多播组。该页面的每个条目包括三部分：VID，多播MAC地址和端口列表。VID和多播MAC地址是条目的索引。

一个端口可以不是多播组的成员，可以是多播组的成员。在页面的端口上的字符含义如下表16-5：

表16-5：

字符	全称	含义
-	Non-member	该端口不是这个VLAN的成员
M	Member	该端口是这个VLAN的tagged成员



图16-23 当前多播组配置页面

（4）静态多播组配置页面

图16-24是静态多播组配置页面，该页面允许用户创建一个多播组和配置一个多播组的端口成员。该页面由两部分构成：活动行和列表框。活动行在首行，可编辑，活动行下方的列表框包含一系列的以VID和MAC地址标识的静态多播组。



图16-24 静态多播组配置页面

如果要创建一个新的多播组，用户在活动行输入VID、多播MAC地址及端口列表信息，然后按下应用（Apply）或存储（SAVE）键，这时列表框会显示用户创建的多播组的VID和MAC地址。如果输入的VLAN不存在或输入的MAC地址不是多播MAC地址，此时多播组创建不成功。图16-25是当输入的MAC地址不是多播地址时的错误提示。



图 16-25 错误信息

如果要修改一个已经存在的多播组，用户需要点击列表框中相应的多播组。该多播组将显示在活动行中，用户可以修改该多播组的端口列表信息。当修改结束后，按下应用（APPLY）或存储（Save）键。

如果要删除一个多播组，用户需要点击列表框中相应的多播组。该多播组将显示在活动行中，按下删除（Delete）键可以删除该多播组，同时该多播组的信息将从列表框中去除。

一个端口可以不是多播组的成员，也可以是多播组成员。当修改多播组的端口列表时，在每一个端口处点击鼠标，可以在梂 - 、M 之间进行切换。在页面的端口上的字符含义如前表 16-6。

表 16-6:

字符	全称	含义
-	Non-member	该端口不是这个VLAN的成员
M	Member	该端口是这个VLAN的tagged成员

（5）私有 VLAN 配置页面

图 16-26 是私有 VLAN 配置页面，用户通过该页面可以对一个私有 VLAN 组的 VLAN 和端口进行配置。iSpirit2924G/2924F 交换机支持 12 个私有 VLAN 组，配置私有 VLAN 时首先要选择私有 VLAN 组号，然后对该私有 VLAN 组的 VLAN 和端口进行配置。

在私有 VLAN 组的 VLAN 和端口信息都配置好后，按下应用（APPLY）或存储（Save）键，如果私有 VLAN 组配置成功，则该私有 VLAN 组的状态是 active，否则，私有 VLAN 组的状态会显示失败的原因。当要删除私有 VLAN 组时，选择私有 VLAN 组号后直接按下删除（Delete）键即可。



图 16-26 私有 VLAN 配置页面

7.堆叠配置

（1）堆叠配置页面

图 16-27 是堆叠配置页面，用来设置堆叠状态，协议 hello 时间，堆叠名称，堆叠端口等。



图 16-27 堆叠配置页面

（2）成员管理页面

图 16-28 是堆叠成员管理页面。当本交换机是命令交换机时，显示堆叠成员和堆叠侯选成员，可以通过此页面使堆叠侯选成员成为堆叠成员，也可以通过此页面是堆叠成员成为侯选成员。

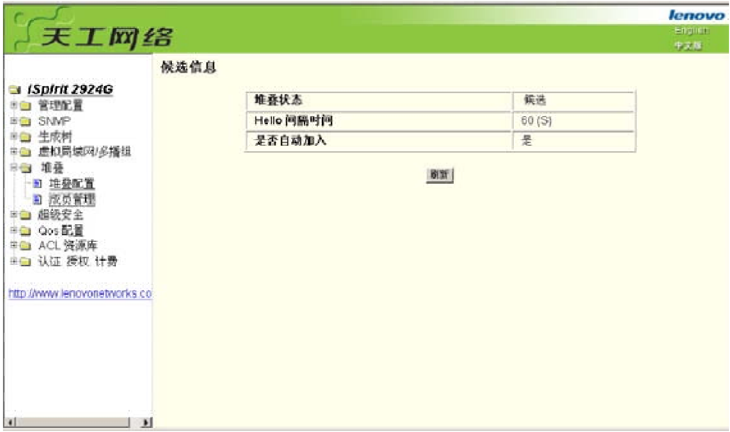


图 16-28 堆叠成员管理页面

8.超级安全配置

（1）MAC 地址手工绑定配置页面

图 16-29 是 MAC 地址手工绑定配置页面，该页面允许用户在一个端口上绑定一个或多个 MAC 地址（最多可绑定 128 个），只允许绑定的 MAC 地址的主机通过此端口访问网络，而不允许未绑定的 MAC 地址的主机通过此端口访问网络。

当用户要做 MAC 地址绑定时，首先选择要绑定 MAC 地址的端口，在该端口下可以手工输入 VLAN 号和 MAC 地址与端口进行绑定。当页面上表中没有条目时，表明该端口此时没有做 MAC 地址绑定，当表中有一个或多个条目时，表明该端口已经做了 MAC 地址绑定。

当用户需要为该端口解绑定时，可以对想要解绑定 MAC 地址项前的小方框打上钩号，然后点击解绑定按钮即可实现解绑定。如果想对该端口下所有的 MAC 地址解绑定，则可以点击全选按钮，然后选择解绑定按钮。在绑定一个 MAC 地址时，如果输入的 MAC 地址错误，系统会弹出警告信息，提示用户输入的 MAC 地址出错。



图 16-29 MAC 地址手工绑定配置页面

（2）MAC 地址自动绑定配置页面

图 16-30 是 MAC 地址自动绑定配置页面，该页面允许用户对一个端口上学习到的 MAC 地址自动与该端口进行绑定。当端口做了 MAC 地址绑定后，只允许绑定的 MAC 地址的主机通过此端口访问网络，而不允许未绑定的 MAC 地址的主机通过此端口访问网络。

当用户要做 MAC 地址绑定时，首先选择要绑定 MAC 地址的端口，如果该端口已经做了 MAC 地址绑定，那表中的条目前没有小方框。如果该端口没有做 MAC 地址绑定，系统会把该端口学习到的 MAC 地址列在表中，每个条目前有一个小方框。此时用户可以在要绑定的 MAC 地址项前的小方框打上钩号，选择绑定按钮就可以进行 MAC 地址绑定。如果用户想对学习到的所有 MAC 地址进行绑定，则可以点击全选按钮，然后选择绑定按钮。端口自动绑定了 MAC 地址后的页面如图 16-30 所示。

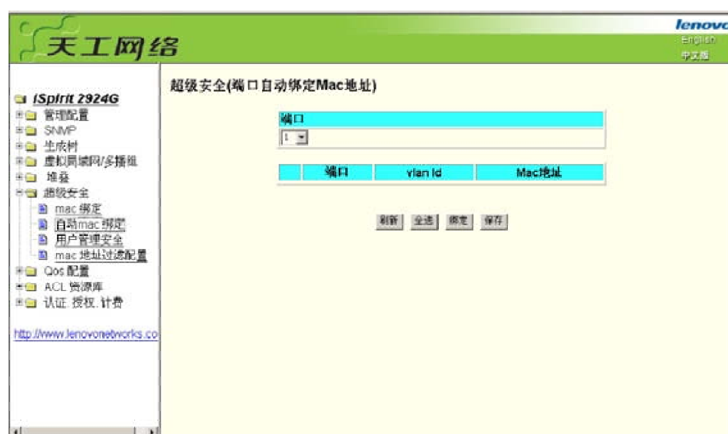


图 16-30 MAC 地址自动绑定配置页面

（3）用户管理安全配置页面

图 16-31 是用户管理安全配置页面，通过该页面的配置，管理员可以对网管服务 TELNET、WEB 和 SNMP 进行控制，可以打开或关闭这些服务，可以把这些服务与 IP 标准的 ACL 组挂接起来，控制主机对这些服务的访问。

交换机缺省情况下 TELNET、WEB 和 SNMP 服务是打开的，并且不做 ACL 过滤，也就是所有的主机都可以访问交换机的这三种服务。如果管理员为了安全性，不想给别的用户提供其中的一种或几种服务，可以把其中的一种或几种服务关闭。如果管理员只希望特定的主机可以访问其中的一种或几种服务，可以把其中的一种或几种服务做 ACL 过滤。

当某服务要做 ACL 过滤时，需要打开这个服务，并且要选择一个 IP 标准的 ACL 组，此时该 ACL 组必须存

在，并且状态必须是 active。

需要注意的是，如果管理员在此页面上控制 WEB 服务（比如关闭 WEB 服务）可能使用户不能再使用 WEB 页面，此时 WEB 页面会变为灰色，这时可以通过其他方式登陆交换机并控制 WEB 服务使用户可以使用 WEB 页面（如打开 W E B 服务）。



图 16-31　用户管理安全配置页面

（4）M A C 地址过滤配置页面

图 16-32 是 MAC 地址过滤配置页面。ISpirit2924G 交换机可以根据报文的目的地址进行过滤。

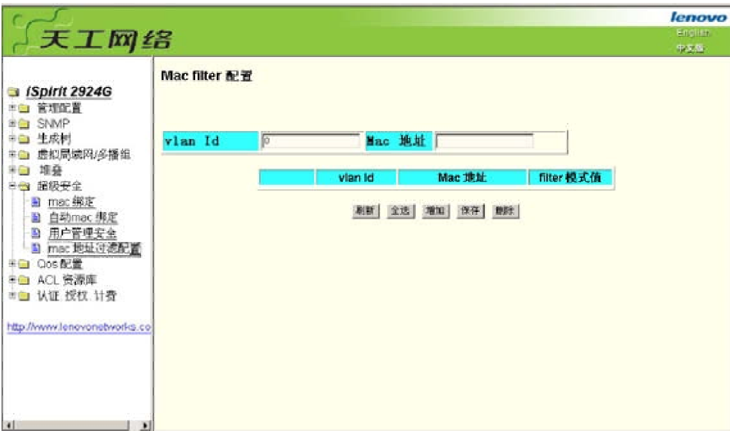


图 16-32　MAC 地址过滤配置页面

9.QoS 配置

（1）C O S 值到输出队列映射配置页面

图 16-33 是 COS 值到输出队列映射配置页面，用户可以通过此页面设置 COS 值和输出队列的映射关系。



图 16-33　COS 值到输出队列映射配置页面

（2）Ip　precedence 值到输出队列映射配置页面

图 16-34 是 ip precedence 值到输出队列映射配置页面，用户可以通过此页面设置 ip precedence 值和输出队列的映射关系。

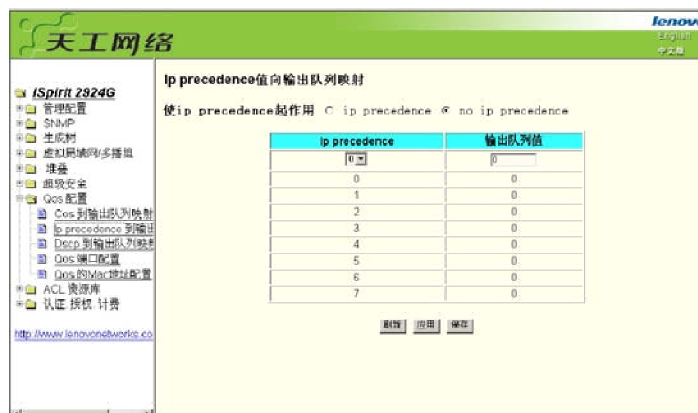


图 16-34　ip precedence 值到输出队列映射配置页面

（3）　DSCP 到输出队列映射配置页面

图 16-35 是 DSCP 值到输出队列映射配置页面，用户可以通过此页面设置 DSCP 值和输出队列的映射关系。



图 16-35　DSCP 值到输出队列映射配置页面

（4）端口 QoS 配置页面

图 16-36 是端口的输出队列配置页面，用户可以通过此页面设置端口的输出队列。



图 16-36　端口的输出队列配置页面

（5）QoS　MAC 配置页面

图 16-37 是 QoS MAC 配置页面,用于配置 MAC 地址的优先级模式，对于包含此 MAC 地址的报文，根据配置模式，将此报文送到最高优先级输出队列。



图 16-37 QoS MAC 配置页面

10.ACL 资然库配置

（1）ACL 标准 IP 配置页面

图 16-38 是 ACL 标准 IP 配置页面，用户可以通过此页面建立 ACL 标准 IP 的规则库。用户可以选择一个 ACL 组号（范围在 1-199 之间），在该组中创建一条或多条规则（总共一个组内可以支持 128 条规则）。在一条规则中可以匹配的字段只有源 IP 地址（可带掩码）。

用户在配置规则时，每一个规则都必须有一个过滤模式，过滤模式包括四种：允许、拒绝、全部允许和全部拒绝。如果用户选择了“全部允许”和“全部拒绝”时，配置的源 IP 地址将不起作用，统一表示为：0.0.0.0，掩码 255.255.255.255。当用户不配置任何字段，即都为空时，此时“拒绝”相当于“全部拒绝”，而“允许”相当于“全部允许”。

页面上的每一组规则都有一个引用计数，该字段是只读的，不能进行配置。该字段提示用户当前有多少应用在使用这组规则，使用规则的应用有 ACL 过滤、QoS 业务类和用户管理安全。当引用计数为 0 时，表明没

有应用使用此组规则，此时可以对这组规则进行配置，如增加规则，删除规则，修改规则。当引用计数非 0 时，不能对这组规则进行配置。

用户在创建一个规则组中的一条规则时，系统会自动给该条规则一个规则号，当删除一个规则组中的一条规则时，别的规则的规则号不变。系统会自动给一个规则组中的规则进行排序。

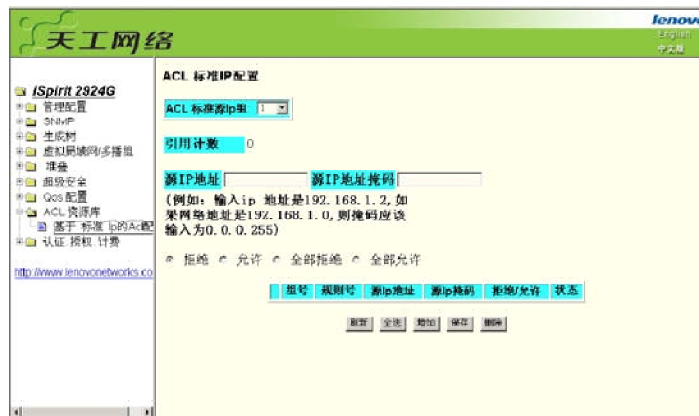


图 16-38 ACL 标准 IP 配置页面

11.认证.授权.计费（AAA）配置

（1）RADIUS 配置页面

图 16-39 是 RADIUS 配置页面，用户可以配置与 RADIUS 相关的信息，可设置的信息包括：

RADIUS 服务器的 IP 地址，在做认证计费时一定要设置此字段。

备用 RADIUS 服务器的 IP 地址，如果有备用 RADIUS 服务器时可以设置此字段。

认证 UDP 端口，默认值为 1812，用户一般不需要修改此字段。

是否启动计费，默认是启动的，在做认证计费时一般要启动计费。

计费 UDP 端口，默认值为 1813，用户一般不需要修改此字段。

共享密钥，用来设定交换机与 RADIUS 服务器之间的加密共享密码，在做认证计费时一定要设置此字段，并且要与 RADIUS 服务器上的设置一样。

厂商特定信息，用户一般不需要修改此字段。

NAS 端口、NAS 端口类型、NAS 服务类型，这三个值用户一般不用做修改。



图 16-39 RADIUS 配置页面

（2）802.1x 配置页面

图 16-40 是 802.1x 配置页面，用户可以通过此页面配置 802.1x 相关的一些信息，主要包括：

是否启动 802.1x 协议，在做认证计费时一定要启动 802.1x 协议。

是否打开重新认证功能，缺省没有打开，在做认证计费时根据实际情况来决定。打开重新认证功能会使用户在使用认证计费时更可靠，但会稍微加大网络的流量。

设置重新认证时间间隔，只有在重新认证功能打开的情况下才有效，缺省是 3600 秒，在做认证计费时根据实际情况来设定该值，但该值不要太小。

Quiet Period 定时器，用户一般不需要修改此字段。

Tx-Period 定时器，用户一般不需要修改此字段。

Server timeout 定时器，用户一般不需要修改此字段。

supplicant timeout 定时器，用户一般不需要修改此字段。

Max Request 个数，用户一般不需要修改此字段。

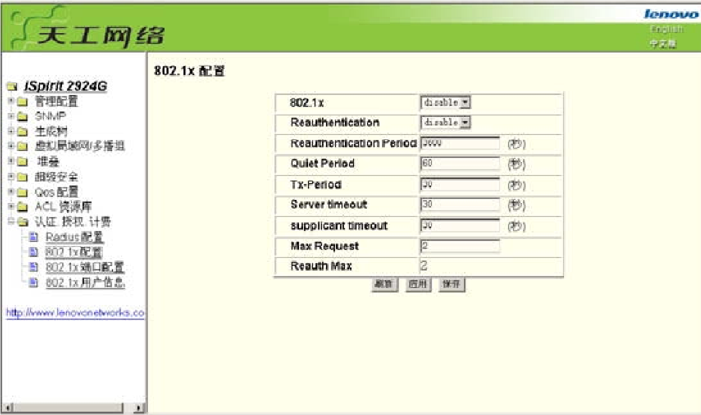


图 16-40　802.1x 配置页面

（3）802.1x 端口配置页面

图 16-41 是 802.1x 端口配置页面，用户通过此页面可以对 802.1x 端口状态和支持的最大主机个数进行配置，同时可以查看各个端口的 802.1x 配置情况。802.1x 端口状态包括四种类型：N/A 状态、Auto 状态、Force-authorized 状态和 Force-unauthorized 状态。当某端口需要做 802.1x 认证时，要把该端口设置为 Auto 状态，如果不做认证就可以访问网络，把该端口设置为 N/A 状态，其它两个状态在实际应用中很少用到。

在做 802.1x 认证时，端口缺省接入的最大主机数是 9 个，用户可以修改此字段，最大可以支持到 250 个。



图 16-41　802.1x 端口配置页面

（4）802.1x 用户显示页面

图 16-42 是 802.1x 用户显示页面，用户可以通过此页面查看某端口下接入的所有用户的状态，可以时时查看到认证的用户的信息。



图 16-42　802.1x 用户显示页面

附录 A 产品特征参数

此部份详细说明 iSpirit 2924G/2924F **交换机的运行环境。**

接口	
10Base-T/100Base-TX RJ-45 UTP-5 **端口**	
1000Base-X **端口**	
扩展插槽	
UART **控制端口**	
物理特点	
重量：5KG	
2924G **尺寸：**444mm × 44.45mm × 266mm(W × H × L)	
2924F **尺寸：**444mm × 44.45mm × 361mm(W × H × L)	
环境要求	
温度	**操作:** 0⁰C to 40⁰C (32⁰F to 104⁰F)
	存储: -20⁰C to 70⁰C (-4⁰F to 158⁰F)
湿度	**操作:** 10% to 90% RH
	存储: 5% to 90% RH
海拔	**操作:最高** 3000 **米**(10,000 **英尺**)
	存储:最高 4570 **米**(15,000 **英尺**)
网络媒体	
10Base-T:	UTP Category 3, Category 4 **或** Category 5 **网线**
100Base-TX:	UTP Category 5 **网线**
1000Base-X:	1000Base-SX,1000Base-LX/LH **或** 1000Base-ZX **光纤**
10/100/1000Base-T:	UTP Category 5 **网线** **或** UTP Category 5 Enhanced **网线**
控制端口：	**专用串口线**
电源要求	
电压范围	180-264V **交流电源输入**
电流限制	**最大** 1.5A

表 A-1 **联想天工** iSpirit 2924G/2924F **交换机产品技术指标**

附录 B 接口与网线的技术说明

此部份说明联想天工 iSpirit 2924G/2924F **交换机网口和网线的技术特征。**

接口说明

10/100Base-T 端口

10/100Base-T 以太网端口使用标准 RJ-45 接头。端口的发送信号（TD）和接收信号（RD）内部交叉。由交换机实现直连网线与交叉网线的自协商，所以与这些端口连接时可以使用直连网线或交叉网线。

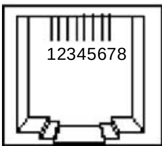


图 B-1 10/100Base-T 端口的管脚排列

10/100/1000Base-T 端口

10/100/1000 Base-T 端口使用标准 RJ-45 接口和内部交叉的引脚排列方式。这些端口的发送信号（TD）和接收信号（RD）内部交叉。内部硬件实现直连网线与交叉网线的自协商，所以与这些端口连接时可以使用直连网线或交叉网线。10/100/1000Base-T 端口的管脚如图 B-1 所示。

控制端口

交换机控制端口使用标准的 9 针 UART 接口。UART 接口的管脚如图 B-2 所示。

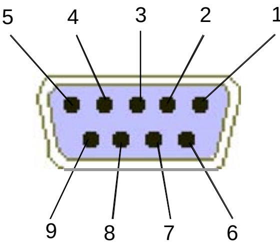


图 B-2 UART 接口的管脚

控制端口专用电缆的管脚说明如表 B-3 所示。

表 B-3 控制端口专用电缆的管脚说明:

电缆一端信号	DB-9 管脚	DB-9 管脚	电缆另一端信号
DCD	1	1	DCD
RXD	2	3	TXD
TXD	3	2	RXD
DTR	4	4	DTR
SIG GND	5	5	SIG GND
DSR	6	6	DSR
RTS	7	7	RTS
CTS	8	8	CTS
RI	9	9	RI

网线说明

交叉和直连双绞线管脚说明

1.直连和交叉双绞线管脚示意图如 B-3 所示。

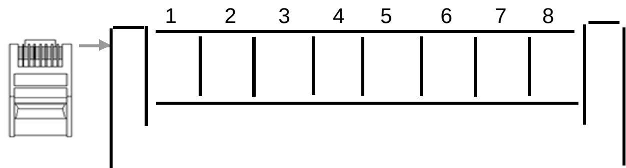


图 B-3 RJ-45 双绞线管脚示意图

2.直连双绞线的国际标准

直接连结双绞线的接线方法的国际标准如图 B-4 所示，其主要特点是，双绞线两头 SIDE1、SIDE2 两方的接线顺序一样，并且接到 RJ-45 头 3、6 针上的是同一对双绞线。

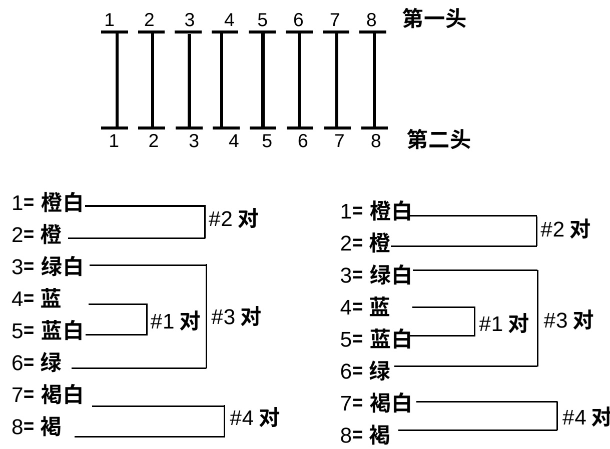


图 B-4 RJ-45 直连双绞线的国际标准

3.交叉对连双绞线的国际标准

交叉对连双绞线的接线方法的国际标准如图 B-5 所示，其主要特点是，双绞线两头 SIDE1、SIDE2 两方的接线顺序不一样，其连接如下图所示。

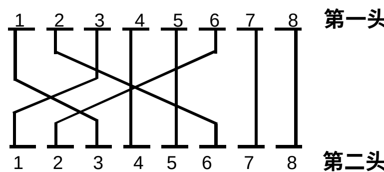


图 B-5 RJ-45 交叉对连双绞线的国际标准



图 B-5 续 RJ-45 交叉对连双绞线的国际标准